Harmonisation of cybercrime law

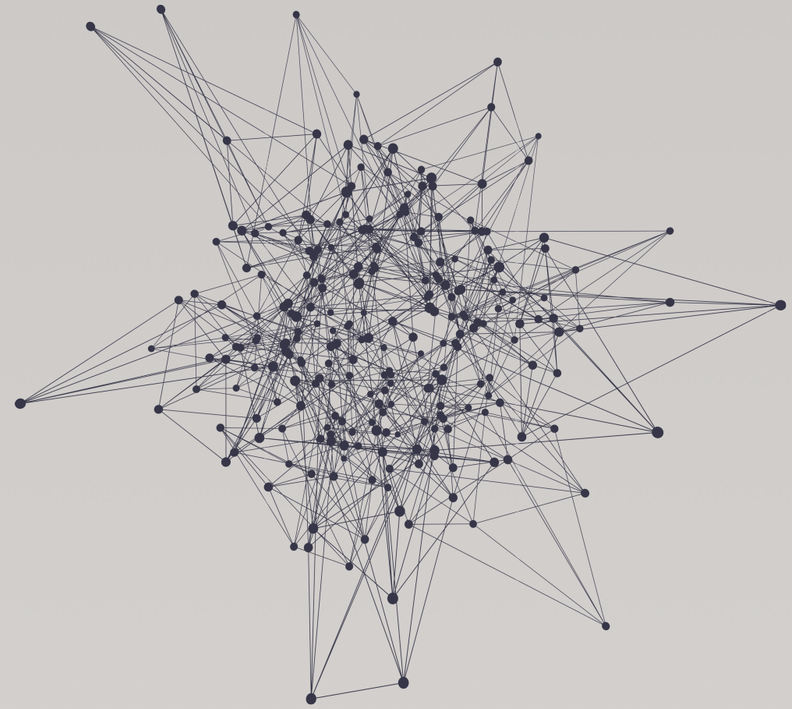
Past solutions, present tensions, and future challenges

Bussolati, N.

Publication date
2020

Document Version
Final published version

License
Other



Harmonization of Cybercrime Law

Past Solutions, Present Tensions, and Future Challenges

Nicolò Bussolati

UNIVERSITY OF AMSTERDAM
AMSTERDAM CENTER FOR INTERNATIONAL LAW
FACULTY OF LAW

HARMONIZATION OF CYBERCRIME LAW
Past Solutions, Present Tensions, and Future Challenges
N. Bussolati

Harmonisation of Cybercrime Law
Past Solutions, Present Tensions, and Future Challenges

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op woensdag 21 oktober 2020, te 10.00 uur
door Nicolo Bussolati
geboren te Torino

Promotiecommissie

Promotor:	prof. mr. dr. H.G. van der Wilt	Universiteit van Amsterdam
Copromotores:	prof. dr. G.Y.J.M. Mettraux	Universiteit van Amsterdam
	prof. dr. M. Papa	Università degli studi di Firenze
Overige leden:	prof. dr. D. Abels	Universiteit van Amsterdam
	prof. mr. T. Blom	Universiteit van Amsterdam
	prof. dr. P.A.L. Ducheine	Universiteit van Amsterdam
	prof. dr. I. Bantekas	Hamad Bin Khalifa University
	prof. dr. P. Gaeta	Graduate Institute Geneva

Faculteit der Rechtsgeleerdheid

…cercare e saper riconoscere chi e cosa,
in mezzo all'inferno, non è inferno,
e farlo durare, e dargli spazio.

LIST OF ABBREVIATIONS

CoE	Council of Europe
CJEU	Court of Justice of the European Union
CUP	Cambridge University Press
DoS	Denial of Service (attack)
ECFR	European Charter of Fundamental Rights
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EIO	European Investigation Order
EU	European Union
FR	France
GER	Germany
ISP	Internet Service Provider
ITC	Information Technology Company
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
ISO	International Organization for Standardisation
ITA	Italy
ITU	International Telecommunication Union
IRC	Internet Relay Chat
LAS	League of Arab States
LOIC	Low Orbit Ion Cannon
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OUP	Oxford University Press
RICO	Racketeer Influenced and Corrupt Organizations (Act)
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
UN GA	United Nations General Assembly

UNODC	United Nations Office on Drugs and Crime
UK	United Kingdom
US	United States of America

TABLE OF CONTENT

I INTRODUCTION

"Iha Śāriputro rūpam śūnyatā, śūnyataiva rūpam rūpānna prthak śūnyatā, śūnyatāyā na prthag rūpam yadrūpam sā śūnyatā, yā śūnyatā tadrūpam evam vedanāsamjñāsamskāravijñānāni"[1]

[1] Prajñāpāramitā Hrdaya sūtra III 9-16: "Here, Sariputra, form is emptiness and emptiness is form. Emptiness does not differ from form, form does not differ from emptiness. Whatever is form, that is emptiness, whatever is emptiness, that is form. The same thing for sensations, perceptions, impulses, and consciousness."

I.I. A BRIEF HISTORY OF CYBERCRIME.

One of the most significant features of humanity, which differentiate man from most animals,[2] is the capacity to craft tools to overstep limits imposed by nature.[3] At first, such tools were simple devices. Gradually thereafter, the evolution of science and technology expanded their capacities. Finally, humans created machines able to mimic not only their arm, but also their mind.

The computer was the first artificial apparatus able to receive instructions (programs) and process them. In the beginning, computers were capable only of performing relatively simple calculations.[4] Following an exponential technologisation,[5] computers became faster and able to execute a higher number of instructions. Development in hardware and software improved the features and functions of computers, which became increasingly more precise and sophisticated. Rapidly, the new technology proliferated, gaining widespread diffusion, and finding a massive, irreplaceable use in society, particularly in industry, communications, defence, and public and private infrastructures (e.g. finance, politics, health-care).[6] The history of cybercrime begins here.[7]

With the commercialisation of the "personal computer", the binary code diffused into the life of the common people. Digital technology was no longer limited to "insiders" (mainly scientists and

---

[2] Actually, several animals make use of external objects as a "functional extension of mouth or beak, hand or claw, in the attainment of an immediate goal" (J. Van Lawick-Goodall, 'Tool-using in primates and other vertebrates' in D. S. Lehrman, R. Hinde, E. Shaw (eds) *Advances in the Study of Behavior, Vol. 3* (Academic Press, 1970), 195). See, *ex plurimis*, R. W. Shumaker, K. R. Walkup, B. B. Beck, *Animal Tool Behavior: The Use and Manufacture of Tools by Animals* (The Johns Hopkins University Press 2011).

[3] For the history of technology, see, *inter alia*, L. Mumford, *Technics and Civilization* (The University of Chicago Press 2010).

[4] See, e.g., ENIAC (Electronic Numerical Integrator and Computer), the first electronic general-purpose computer, was designed in the mid-forties to calculate artillery firing tables.

[5] The so-called "accelerating change".

[6] See, *inter alia*, R. E. McGinn, *Science, Technology, and Society* (Prentice Hall1991).

[7] Alongside the generic terms "computer crime" and "cybercrime" it is possible to highlight the use by academics of various terms such as: computer-related crime, digital crime, information technology crime, Internet crime, virtual crime, electronic crime and netcrime (see K. Jaishankar, 'Victimization in the Cyberspace: Patterns and Trends', in S. Manacorda (eds), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 92-93. See also U. Sieber, 'Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law', in M. Delmas-Marty, M. Pieth and U. Sieber (eds), *Les Chemins de l'Harmonisation Pénale/Harmonising Criminal Law* (Société de législation comparée 2008). Evidently, the terms "computer crime", "cybercrime", "information technology crime" and "computer-related crime" encompass new digital technologies as an element of the crime, while the other terms are meant to encompass the Internet or inter-computer connections as necessary elements. Moreover, all the terms cover both crimes directed against digital technologies and crimes committed with the assistance of or by means of digital technologies.

information technology students). Laypeople learnt to program computers and use them for various purposes, both legal and illegal.

In particular, new technologies became instruments of crime. They were used as a *medium*, a vehicle between the criminal and the victim; or as a functional extension of the actor's arm, to augment his/her criminal abilities (cybercrime as a crime committed with the assistance or by means of digital technologies).[8]

At the same time, technology became a container of political, cultural, and economic values. The Internet sharply intensified this process of "digitalisation". Digital districts of private houses, banks, government buildings and libraries were edified on servers. In these structures, a "door" could be defective, heedlessly left open, or forcibly penetrated.[9] New technologies became a target for criminals (cybercrime as a crime directed against digital technologies).[10]

Notwithstanding their complexity, digital technologies are a product of the human hand and mind, necessarily affected by certain imperfections. So far, their lack of intelligence and inanimate stupidity makes them relatively easy to deceive or exploit for illegal purposes.

Conditioned by the dynamic variability of its technological component, cybercrime shaped its forms and modalities alongside technological evolution. Variations mainly followed three key markers: the technology used to perform the act; the technology at which the act is targeted; the technology used as a link between the act and the target. A diachronic analysis of cybercrime, rationalised around these factors, highlights four main phases.

The first phase is antecedent to the diffusion of the personal computer. The targets of the crime were mainly computerised systems of the public or private sector. For instance, in the '70s, the so-called "phone phreaks" manipulated the computerised communication system of telephone companies. They hacked the phone network, largely to be able to make free long-distance calls.[11] The technology used to perform the act was the telephone. The target was the computer controlling the phone network. The communication channel between the offender and the "victim" was the

---

[8] See, e.g., M. D. Goodman and S. W. Brenner, 'The Emerging Consensus on Criminal Conducts in Cyberspace' (2002) 10 IJLIT 139, 144-145.

[9] According to the Internet Engineering Task Force, which develops and promotes Internet standards, a vulnerability is a "flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy" (Internet Engineering Task Force, RFC (Internet Security Glossary) 2828 <https://tools.ietf.org/html/rfc4949>).

[10] See M. D. Goodman and S. W. Brenner, 'The Emerging Consensus on Criminal Conducts in Cyberspace' (n 8).

[11] See, e.g., A. Hoffman, *Hacking Ma Bell: The First Hacker Newsletter – Youth International Party Line, The First Three Years* (Warcry Communications 2010); B. Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (Bantam Books 1992).

phone network itself. In this first phase, however, cybercrime's diffusion and significance were still limited.

The second phase is related to the commercialisation, personalisation, and diffusion of computers. These devices are now powerful criminal tools and targets of crime. The diffusion of technical knowledge and skills radically augmented. Malware[12] were created and diffused.[13] The technical features of the computer and its broad distribution brought new types of offences aided by or perpetrated on computers: crimes against property – frauds, thefts and piracy – and crimes against the confidentiality, integrity, and availability of computer systems and data.[14] At an exponential rate, the computer gained a central role in society through its "personalisation", and the "computerisation" of many (public or private) critical infrastructures. The potentialities of new technologies to be both exploitable victim and executioner became evident.[15]

The third phase began in the 1990s, with the global connectivity revolution of the Internet. Inter-computer networks made cybercrime easier, faster, and more dangerous. Furthermore, they made it virulently diffused, and typically transnational. Cybercrime is now deeply immersed in a virtual space that answers to different rules from the physical world and erodes the importance of traditional geopolitical barriers: the so called "cyberspace"[16].

---

[12] Malware (a portmanteau of malicious software) is a software intentionally designed to perform malicious activities against computer systems or data. Malware is a generic term and comprises various types of malicious software, classified according to the activity they perform, such as viruses, worms, Trojan horses, ransomware, spyware, or adware.

[13] See E. Skoudis, *Malware: Fighting Malicious Code* (Prentice Hall 2004), 29ff.

[14] See R. T. Slivka and J. W. Darrow, 'Methods and Problems in Computer Security' (1976) 5 Rutgers Journal of Computers and the Law 217. For instance, in 1981 Ian Murphy (a.k.a. Captain Zap, possibly the first person to be tried and convicted for computer crimes), broke into AT&T's computers changing the internal clocks that measured billing rates. As a result, people were getting discount rates for their calls (see: 'Capitain Zap' (Hack Story, 2011) <http://hackstory.net/Captain_Zap>).

[15] See E. A. Glynn, 'Computer Abuse: The Emerging Crime and the Need for Legislation' (1983) 12 Fordham Urban Law Journal 173.

[16] The word "cyberspace" began to be used in science fiction literature (in particular "cyberpunk") in the '80s. One of the first uses of the word is found in William Gibson's"Neuromancer". In this book, Gibson defines cyberspace as a "consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding" (W. Gibson, *Neuromancer* (Ace 1984) 51). Indeed, part of the term's vast success is due to its vagueness, as a term that was able to comprehend new perceptions of space induced by the new technologies. Accordingly, cyberspace has been defined as "the diverse experiences of space associated with computing and related technologies" (Lance Strate, 'The varieties of cyberspace: Problems in definition and delimitation' (1999) 63 Western Journal of Communication 382, 383). As the Internet evolved, the spatial conception of cyberspace acquired a more stable meaning of a "place", since people virtually met there, stored data and opened their commercial activities. Alongside the ontological level of cyberspace as an *alter-space*, the term may be intended as the physical apparati that constitutes the virtual space (physical cyberspace), such as computers, cables, servers (R. J. Gozzi, 'The cyberspace metaphor'(1994) 51 ETC: A Review of General Semantics 218).

Cyberspace is a web of connected servers and machines, which creates a virtual space covering and permeating the physical world. It is based on a theoretical architecture weaved on entirely new concepts of time and space. Everything and everyone on the web, even technology-dependent State's critical infrastructures, may be only a "click" away.

Cybercrime has now entered a fourth phase, whose exact frontiers have not yet been fully manifested. The widespread diffusion of fast cellular mobile communications and Wi-Fi hotspots created a constant and diffused connection to the web, and a continuous incoming and outgoing traffic of data. According to analysts, in 2018, the number of connected devices worldwide exceeded 17 billion.[17] Computing and communication capabilities are increasingly integrated into all kinds of objects, creating human-to-machine and machine-to-machine complex networks of interrelation. The information network is going towards an Internet-of-Things scenario.[18] Critical infrastructures are increasingly controlled by embedded computers and networks (the so-called cyber-physical system).[19] Metropolises are becoming "smart". Technological cities, where digital services – such as Wi-Fi hotspots, smart energy grids, surveillance systems and intelligent transportation systems[20] – communicate and interact between them and with interconnected citizens, are now commonplace. Physical and digital spaces are melting into a new hybrid-space.[21] Such transformations will induce radical sociological changes and new augmented issues related to security, privacy, and crime.

Furthermore, the "artificial intelligence" technology is progressing rapidly. Artificially created, technologically intelligent agents will eventually be capable of deduction, reasoning, and different

---

17 See K. Lasse Lueth, 'State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating' (IOT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>.

18 See I. Saleh, M. Ammi and S. Szoniecky (eds), *Challenges of the Internet of Things: Technique, Use, Ethics* (John Wiley & Sons, 2018).

19 See H. Song, D. B. Rawat, S. Jeschke, C. Brecher and M. Kaufmann (eds) *Cyber-Physical Systems: Foundations, Principles and Applications* (Elsevier 2016). For instance, several American critical infrastructures are controlled by a Supervisory Control and Data Acquisition Diffusion (SCADA) system, a computer-control system that manages and controls physical processes.

20 See Symantec, *Executive Report: Smart Cities. Transformational 'Smart Cities': Cyber Security And Resilience* (2013); A. AlDairi, 'Cyber Security Attacks on Smart Cities and Associated Mobile Technologies' (2017) Procedia Computer Science 1086.

21 See A. de Souza e Silva, 'From Cyber to Hybrid Mobile Technologies as Interfaces of Hybrid Spaces' (2006) 9 Space and Culture 261; E. Kluitenberg, S. Sassen, H. Rheingold, K. Brams, D. Pultau, *Open 11: Hybrid Space* (Nai Uitgevers Pub 2006).

responses according to situations (using evaluations based on experience and even ethical principles[22]).[23]

It is fascinating to consider how crime and legal systems will react to artificial intelligence. An intelligent machine could be more difficult to "mislead". Illegal access to computer systems may become more similar to fraud than to trespass. Still, the future of cyber-law may be tied to the direction taken by artificial intelligence.

Will humans create machines that are a pale simulation of the human mind, an *analogon*, a mechanical equivalent?[24] If so, human-to-machine and machine-to-machine relations will tend towards the norms that today regulate human relations.

Will the future intelligent machine be conceived as an *aliud*: not an instrument or a reflection of the human hand and mind, but a solution to human faultiness and emotional instability (consider a machine-judge, equally, and strictly applying the law in judicial decision-making[25])? Will we trust machines even more than humans, granting them the power to take important decisions without an eventual human interaction or intervention?[26] If so, it might be interesting to see if cyberlaw would be enriched by a new genus of law regulating human-to-machine relations.

Will the rise of an era of hyper-reality, and the loss of human referentiality in favour of the machine,[27] transform every act of hacking into an act of resistance against the new artificial gods? Yet, the word "cybernetics" comes from the Greek *κυβερνάω*: to govern, to direct.

---

[22] See, inter alia, P. Lin, 'Why ethics matters for autonomous cars' in M. Maurer, J. C. Gerdes, B. Lenz, H. Winner (eds) *Autonomous Driving* (Springer 2016) 69.

[23] About artificial intelligence, see, inter alia: P. C. Jackson, *Introduction to artificial intelligence* (Courier Dover Publications 2019). Alan Turing, one of the most renowned fathers of computer science, was fascinated by the idea of a thinking machine capable of using logic, probabilities, learning and background knowledge. .

[24] See J. Baudrillard, *L'echange symbolique et la mort* (Gallimard 1976).

[25] See: A. D'amato, 'Can/Should Computers Replace Judges?' (1977) 1 Georgia Law Review 1277; R. M. Re and A. Solow-Niederman, 'Developing Artificially Intelligent Justice' (2019) 22 Stanford Technology Law Review 242.

[26] Consider unmanned cyber defences automatically responding to cyberattacks given the satisfaction of programmed conditions.

[27] See: J. Baudrillard, *Simulacra and Simulations – XIII. Simulacra and Science Fiction* (Éditions Galilée 1981) <http://www.egs.edu/faculty/jean-baudrillard/articles/simulacra-and-simulations-xiii-simulacra-and-science-fiction/>.

I.II. EARLY ANSWERS TO NEW TECHNOLOGY CRIMES.

In the 1970s, the academic community began to show interest on the present and future implications of new technology for criminal law. The first researches on crimes involving the use of computers and the illegal exploitation of the loopholes in hardware and software were published.[28] The attention of the legislator was then attracted by the increasing cases of virus infections, hacker attacks on public computerised systems, and political espionage (such as the attack through ARPANET and MILNET[29] networks on US military computers by German hackers and the subsequent selling of data to the KGB)[30]. These cases underlined the real extent of the phenomenon, the vulnerability of the new information society, and the need for a tailored legislative response.[31]

I.II.I. DOMESTIC REFORMS.

In 1977, the US Senate's Committee on Government Operation, led by Senator Abraham Ribicoff, published a comprehensive study on computer crimes and recommended a series of "corrective actions" to the government.[32] The study was principally focused on cyberattacks against government infrastructures. It suggested a series of administrative actions aimed at enhancing the security of public computer systems.[33] With regards to possible legislative responses to computer crime, the

---

[28] See D. B. Parker, *Crime by Computer* (Scribner 1976); A. Bequai, *Computer Crime* (Lexington 1978). In Europe, see: U. Sieber, *Computercriminalitat und Strafrecht* (Carl Heymanns Verlag KG 1977); A. Solarz, *Computer Technology and Computer Crime* (National Swedish Council for Crime Prevention, Research and Development Division 1981). In the first period, the academic attention was focused mainly on economic computer crime. In particular, some egregious cases involving significant economic loss drew the attention of the scholars (e.g.: the so called "Equity Founding Fraud" – amounting to 1 to 2 billion dollars – operated through a computer system dedicated to the management of fictitious insurance policies (see: R. Loeffler, *Report of the trustee of the Equity Funding Corporation of America* (1974); R. L. Soble & R. E. Dallos, *The Impossible Dream: The Equity Funding Story* (G.P. Putnam's Sons 1975)).

[29] A section of ARPANET used for unclassified United States Department of Defense traffic.

[30] See C. Stoll, *The Cuckoo's Egg* (Doubleday 1989).

[31] See U. Sieber, *Legal Aspects of Computer-related Crime in the Information Society* (Comcrime Study 1998). See also, generally, on the informational development and social effects of new technology: Y. Masuda, *The Information Society: As Post-industrial Society* (World Future Society 1980); F. Webster, *Theories of Information Society* (Routledge 2007).

[32] US, Committee on Governmental Operations, the 95th Congress 1 Session, *Staff Study of Computer Security in Federal Programs* (United States Senate 1977).

[33] Idem, 276 – 277.

Committee recommended the adoption of legislation "that would prohibit unauthorised use of computers owned by, operated for, under contract with, on behalf of or in conjunction with the US Government", "expand the wire fraud[34] jurisdiction to reach any use of the facilities of wire communications, regardless of whether the actual signal travels interstate", and "clarify definitional guidelines".[35]

The study found that the main problem faced by the existing penal legislation existed around the applicability of the traditional concepts of criminal law to the new technology crimes. In 1977, the study was translated into a legislative proposal (the "Federal Computer System Protection Act"[36]) aimed at criminalising "computer misuse".[37] According to Ribicoff, the "committee investigation revealed that the Government has been hampered in its ability to prosecute computer crime. The reason is that our laws, primarily as embodied in Title 18, have not kept current with the rapidly growing and changing computer technology. Consequently, while prosecutors could, and often did, win convictions in crime by computer cases, they were forced to base their charges on laws that were written for purposes other than computer crime. Prosecutors are forced to 'shoe horn' their cases into already existing laws, when it is more appropriate for them to have a statute relating directly to computer abuses."[38] Ultimately, the proposal was not adopted. However, it acted as a pacemaker for the enactment of cybercrime legislation at the federal level as well as in Arizona and Florida.[39]

The traditional criminal law structure, primarily based on kinetic actions and tangible objects, was confronted with a new set of ethereal concepts, technological elements, and new means of perpetration of the crime. From the early diffusion of computers to mobile devices and cloud technology[40], technological evolution fostered the propagation and increased the dangerousness of particular types of crimes, generated new criminal behaviours, and created a demand for criminal law to protect a new set of values.

---

[34] Committed through telephone lines.

[35] Staff Study of Computer Security in Federal Programs (n 32) 277.

[36] See US, 95th Congress, *Congressional Records* (Vol. 123, No. 111, 1977).

[37] …"knowing, wilful manipulation or attempted manipulation of a computer, computer system, computer network or any part thereof" (see G. D. Baker, 'Trespassers Will Be Prosecuted: Computer Crime in the 1990s' (1993-1994) 12 J. MARSHALL J. COMPUTER & INFO. L. 61, 63 note 15).

[38] US, 95th Congress, *Congressional Records* (n 36), Ribicoff Presentation.

[39] See M. D. Goodman and S. W. Brenner, 'The Emerging Consensus on Criminal Conducts in Cyberspace' (n 8) 162; S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva* (2008) <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.

[40] A cloud is a network of servers that provides services (such as storing, managing and processing computer data) through the use of hardware/software resources distributed through such a network. Cloud servers are located in data centres all over the world and can be accessed from any device via the Internet.

The existing legal framework appeared unable to cover new "cyber" crimes and to protect new digital objects and legal interests. Additionally, an extensive analogical application of the law would have been contrary to the principle of legality and the prohibition of analogy in *malam partem.*

Although this issue will be considered extensively in the following chapter, it will be useful to introduce it here. The example of an act of unauthorised access to a computer system, possibly including the illegal copying of data, will be used as an illustration. Lacking a specific offence, this conduct will be addressed using the traditional penal framework. The resulting partial and fragmented approach will probably be unable to cover the entire harm caused by the conduct. The act of accessing the computer system will not be subsumed under any traditional offences; not even under the crime of trespass, which usually requires that the accused physically enters or remains on the premises in question.[41] Similarly, the act of copying data would not be covered by burglary – which assumes an unauthorised breaking and entering of a physical structure – nor by theft, since the actor does not "deprive"[42] the owner of a good. The conduct could only be partially covered by offences against privacy or intellectual property. Such offences deal with intangible values, and thereby do not present the inherent problems related to the offences that protect physical property.

Although limited, early domestic reforms in this area were thus mainly focused on the substantive inadequacy of traditional criminal provisions to satisfyingly address the key characteristics of cybercrime.[43] Primarily, the reforms addressed the possibilities of illegally collecting, storing, duplicating, and sharing electronic data. They introduced new norms around data protection[44], intellectual property,[45] and illegal content (such as hate speech or illegal pornography)[46]. Furthermore, few new criminal offences were enacted to protect public infrastructures, criminalising illegal access and damage to data, software, and hardware.[47]

---

[41] See, e.g., US, *Model Penal Code,* § 221.2.

[42] See, e.g., UK, *Theft Act 1968*, section 1: "A person is guilty of theft, if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and "thief" and "steal" shall be construed accordingly".

[43] The inability of the traditional criminal law to offer an adequate response to the new technological threats was highlighted, *inter alia*, in 1979 by Interpol, which advocated a reform of the penal legislations aimed to cover the peculiar characteristics of computer crimes (see S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation* (n 39), 3).

[44] *Inter alia*, Sweden, *Data Protection Act – Law n. 289* (1973), US, *Privacy Act – 5 USC §552a* (1974), FR, *Act on Data Processing, Data Files and Individual Liberties – Act 78-17* (1977). See Sieber, *Legal Aspects of Computer-related Crime* (n 31) 24-26.

[45] *Inter alia*, The Philippines, *Presidential Decree n. 49* (1972); US, *Computer Software Copyright Act* (1980); ITA, *Law 406 on Illegal Duplication, Reproduction, Importation, Distribution and Sell of Unauthorized Phonographic Products* (1981). *Id.*, 27-29.

[46] *Inter alia*, UK, *Criminal Justice and Public Order Act* (1994); GER, *Informations- und Kommunikationsdienste-Gesetz* (1997). *Id.*, 30.

[47] *Inter alia*, ITA, *Amendment to Article 420 Penal Code – Attack on Public Utility Infrastructure* (1978), UK, *Forgery and Counterfeiting Act* (1981), GER, *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität* (1986). Id, at 26-27.

A second area of reform related to procedural law.[48] Besides the emergence of new forms of crime, the process of criminal adjudication increasingly relied on electronic evidence. With the diffusion of digital technology, traces of cyber and ordinary crimes began to be stored in hardware or contained in a digital communication between two devices. Specific investigative tools were thus required to gather electronic evidence. In particular, new laws were needed to provide investigative authorities with effective tools aimed at tackling data volubility and avoid their alteration during the investigative operation. Furthermore, new investigative tools were needed to allow for specific technical surveillance of digital communications.

I.II.II. A TRANSNATIONAL RESPONSE TO CYBERCRIME.

With the development of a global network of digital communication, cybercrime acquired a transnational nature. The expanding territorial scope of cybercrime, due to the "steadily increasing communications by telephones, satellites etc., between the different countries", was already noted in 1979, at the Interpol Third Symposium on International Fraud.[49] In the 1980s, purpose-built and spatially limited computer networks (in particular, ARPANET)[50] started to evolve towards widespread infrastructures.[51] In the 1990s, the Internet revolution nullified the geographical distances, warping space and time. It profoundly diminished the relevance of geographical and political barriers, which traditionally contained crimes within state borders. A virtual superstructure was created (cyberspace), through which crimes and criminals were able to move. Indeed, by

---

[48] *Inter alia*, UK, *Police and Criminal Evidence Act* (1984); Denmark, *Act n. 229* (1985), GER, *Poststrukturgesetz* (1984), Art. 4. S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation* (n 39), 30.

[49] See Interpol, *Third INTERPOL Symposium on International Fraud*, 11-13 December 1979, Presentation by S. Schjolberg. A Questionnaire on computer crime and a training seminar for investigators on computer crime followed the symposium (S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation* (n 39), 3).

[50] The Advanced Research Projects Agency Network (ARPANET) may be considered the "progenitor" of the Internet. Its primary use was to connect universities and research laboratories in the US (see, e.g.: M. Hauben, 'Behind the Net: The Untold History of the ARPANET and Computer Science', in M. Hauben and R. Hauben, *Netizens: On the History and Impact of Usenet and the Internet* (Wiley 1998).

[51] See, e.g., B. M. Leiner et al., 'A brief history of the Internet' (2009) 39 ACM SIGCOMM Computer Communication Review 22.

exploiting the "world-wide" structure of the Internet, offenders were easily committing crimes outside their national borders.[52]

The limits of a purely domestic response to cybercrime started to become evident. The scientific and legislative attention was thus dedicated to the need for a harmonised reform of domestic legal systems, a global level of minimum criminalisation, and an effective transnational cooperation.

The "Love Bug case" perfectly exemplifies the issues relevant to the harmonisation of national cybercrime legislations and the need for tight and efficient transnational cooperation. In 2000, the "Love Bug" malware was created. It was the first malware to use social engineering techniques to propagate itself.[53] In ten days, it infected around 50 million computer systems worldwide, and caused an estimated $5 billion worth of damage.[54] Information technology experts traced the origin of the virus back to the Philippines. A US-Philippines joint investigation led to the identification of a former Philippine computer science student as the creator and disseminator of the malware.[55] However, at that time, the Philippine legal system had not contemplated any specific cybercrime legislation. In the investigation and prosecution of transnational cybercrimes – such as the one committed by this Philippine hacker – deficiencies in national legislation may create three orders of problems. Firstly, they may produce a lack of effectiveness in the investigation phase. In the Love Bug case, when the joint investigation team identified the suspect, it requested a search warrant from a magistrate in the Philippines. However, the warrant was issued with enough delay to let the suspect delete relevant evidence.[56] In cybercrime investigations, specific investigative tools, principally aimed at providing a quick response, are a necessary asset. Moreover, as the Philippine criminal legislation did not criminalise the deliberate distribution of viruses, nor illegal access to computer systems, the alleged perpetrator was prosecuted for malicious mischief and credit card fraud. The charges were dismissed due to the difficulties of subsuming his conduct under such

---

[52] Using the words of a European Commission report: "computer related crimes are committed across cyberspace and do not stops at conventional state-borders. They can, in principle, be perpetrated from anywhere and against any computer user in the world. It has been generally recognised that effective action to combat computer-related crime is necessary at both national and international level" (EU, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM/2000/0890, §1.1 2000).

[53] It propagated through a fake "love letter" sent via email, which attracted the attention of the recipient.

[54] See 'LoveBug – the worm that changed the IT security landscape – is ten years old today' (Infosecurity Magazine, 4 May 2010) <http://www.infosecurity-magazine.com/view/9184/lovebug/>.

[55] See M. Goodman, 'International Dimensions of Cybercrime', in S. Ghosh and E. Turrini (eds), *Cybercrimes: A Multidisciplinary Analysis* (Springer 2010), 318.

[56] See Philippines' Laws Complicate Virus Case. (USA Today, 7 June 2000).

offences.[57] Secondly, inefficiencies in legislation may lead to impunity, inducing furtherance of the crime and the creation of safe-havens from which cyber criminals can act safely. Finally, the accused was not extradited due to the lack of the necessary "double criminalisation" of the act in both States involved in the procedure.[58] It is clear then that the lack of harmonisation of cybercrime legislation may seriously hinder the efficiency of transnational cooperation in criminal matters.

---

[57] See S. H. Gana Jr., 'Prosecution of Cyber Crimes through Appropriate Cyber Legislation in the Republic of the Philippines', <http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html>.

[58] Goodman, 'International Dimensions of Cybercrime' (n 55) 318. On the double criminality principle, see *infra* Chapter 4 - Jurisdiction and International Cooperation.

I.III. THE NEED FOR HARMONISATION.

I.III.I. SOFT LAW.

At first, the growing attention to cybercrime at the regional and international level mainly led to the adoption of soft law instruments.

In 1986, the Organisation for Economic Co-operation and Development (OECD) Committee on Information, Communications and Computer Policy published a survey on the existing law applicable to computer crime. The aim was to offer minimum substantial coverage of the phenomenon for stimulating the rapprochement of legal systems.[59] In 1989, the Council of Europe adopted a Recommendation[60] based on the work of a Committee of computer crime experts. Analogously to the work of the OECD, the Recommendation indicated the necessary direction for an effective response to cybercrime. As pointed out therein, "in all the industrialized states, the same phenomena of computer crime have appeared; prosecuting authorities almost everywhere have to contend with similar difficulties in the application of the traditional domestic criminal law to this new form of crime; dramatic cross-border cases demonstrate the increased need for international co-operation".[61] Specifically, the Recommendation undertook a comprehensive survey on the existing substantive[62] and procedural problems, and included a list of offences to be dealt with under a uniform criminal policy. Moreover, the Recommendation analysed the transnational aspects of cybercrime, with a particular focus on jurisdictional problems and the applicability of the existing European conventions on judicial cooperation in criminal matters. Finally, it recommended the harmonisation of domestic systems, and the elaboration of a cybercrime convention. In 1995, a

---

[59] See OECD, *Computer-related criminality: Analysis of Legal Politics in the OECD Area* (ICCP series n. 10, 1986); M. Portnoy and S. Goodman (eds), *Global Initiatives to Secure Cyberspace* (Springer 2009), 5. This survey was based on a study on the international application and harmonisation of computer crime legislation in the member states.

[60] CoE, *Recommendation No. R (89) 9 on Computer-related crime*, adopted by the Committee of Ministers of the Council of Europe, 13 September 1989, and final report on computer-related crime elaborated by the European Committee on Crime Problems.

[61] Id., 20.

[62] It listed the various forms of computer-related crimes, analysing the constituent elements and legal interests protected.

second Recommendation[63] was dedicated to procedural problems, with a particular focus on search and seizure and technical surveillance.

The United Nations (UN) and the OECD played a central role in stimulating harmonisation.[64] The numerous UN resolutions on cybercrime have largely called for the modernisation and guided development of national legislations on this topic.[65] In particular, the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) have promoted various research conferences, studies and agendas on cybercrime.[66] In 1992, the OECD issued the Guidelines for the Security of Information Systems[67], which were revised in 2002 and 2012. The Guidelines were intended to set the standards for a common framework in the fight against cybercrime, stimulate the adoption of adequate sanctions for the misuse of information systems, and foster international cooperation against cybercrime.

Model international legislation has widely stimulated the harmonisation of cybercrime legislations.[68] Model legislation is a flexible and open instrument that can satisfyingly address the needs of the fight against cybercrime.[69] It allows provisions to which only some of the involved States have

---

63 CoE, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology*, adopted by the Committee of Ministers, 11 September 1995.

64 See, *inter alia,* M. D. Goodman and S. W. Brenner, 'The Emerging Consensus on Criminal Conducts in Cyberspace' (n 8), 166 ff.

65 See, *inter alia*, UN GA, *Resolution 55/63, Combating the criminal misuse of information technologies*, 4 December 2000, A/RES/55/63; UN GA, *Resolution 56/121, Combating the criminal misuse of information technologies,* 19 December 2001, A/RES/56/121.

66 See, generally, G. Murray, 'United against Cybercrime: the UNODC/ITU Cybercrime Capacity Building Initiative', in S. Manacorda (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 215; C. Licciardello, 'Fostering International Cooperation on Cybersecurity: a Global Response to a Global Challenge', in S. Manacorda (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 223. Both the agencies are still on the front line of the fight against cybercrime. Of particular interest are the two comprehensive studies on cybercrime published in 2012 and 2013 (ITU, *Understanding Cybercrime: Phenomena, Challanges and Legal Response* (ITU 2012); UNODC, *Comprehensive Study on Cybercrime* (UN 2013)).

67 OECD, *Recommendation of the Council Concerning Guidelines for the Security of Information Systems*, 26 November 1992.

68 See M. Gercke, 'Hard and Soft Law Options in Response to Cybercrime: how to Weave a More Effective Net of Global Responses', in S. Manacorda (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 201-204. In general, the use of model legislation may satisfyingly conform with the peculiar sensibilities perceived in the harmonisation of criminal law, which is one of the fields of law more related to sovereignty and strictly associated to fundamental State societal values, concerns and interests (See: M. D. Dubber, 'Comparative Criminal Law', in M. Reimann and R. Zimmermann (Eds), *Oxford Handbook of Comparative Law* (OUP 2008), 1287, 1289)

69 See M. Gercke, 'Hard and Soft Law Options in Response to Cybercrime' (n 66), 203-204. As the US Model Penal Code experience points out, model legislations may stimulate a soft "voluntary" approximation, avoiding rigid harmonisation and hard transplants that may eventually lead to rejections. See: H. Wechsler, 'Codification of Criminal Law in the United States: The Model Penal Code' (1968) 8 Columbia Law Review 1425, 1427.

agreed[70], aiming to overcome divergences that may hinder the promulgation of a binding instrument. Moreover, it can easily be amended to track technological development.[71]

The first model legislation on cybercrime was proposed by Stanford University, which in 2000 enacted a Draft International Convention to Enhance Protection from Cyber Crime and Terrorism.[72] The scope of this draft convention covered a list of cyber offences, including acts of cyber-terrorism[73], jurisdictional issues, transnational cooperation, and human rights protection. In 2002, the Commonwealth Model Law on Computer and Computer Related Crime was adopted.[74] Model legislations on cybercrime were also adopted by the League of Arab States in 2004[75], by the East African Community in 2008[76], and by the Common Market for Eastern and Southern Africa Organisation in 2011[77]. Following an International Telecommunication Union and European Commission co-funded project, in 2010 and 2011, model legislative texts were implemented in the Caribbean, sub-Saharan Africa and Pacific Island Countries.[78]

---

[70] If envisaged, even in binding instruments a State can make reservations excluding or modifying the legal effect of specific provisions.

[71] See M. Gercke, 'Hard and Soft Law Options in Response to Cybercrime' (n 66), 203-204.

[72] A, D. Sofaer, G, D. Grove and G. D. Wilson, 'Draft International Convention To Enhance Protection from Cyber Crime and Terrorism', in A. D. Sofaer and S. E. Goodman (Eds), *The Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution 2001), 249. See also A. D. Sofaer, 'Toward an International Convention on Cyber', in in A. D. Sofaer and S. E. Goodman (Eds), *The Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution 2001), 221. The Proposal was developed as a follow-up to a Standford Conference on International Cooperation to Combat Cyber Crime and Terrorism.

[73] Defined through a reference to the International conventions on terrorism.

[74] The Commonwealth, *Model Law on Computer and Computer Related Crime* (2017).

[75] League of Arab States, *Model Law on Combating Information Technology Offences* (2004)

[76] East African Community, *Draft Legal Framework for Cyberlaws* (2008)

[77] Common Market for Eastern and Southern Africa, *Cybersecurity Draft Model Bill* (2011)

[78] See *Establishment of Harmonized Policies for the ICT Market in the ACP Countries, Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts* (ITU 2012). These model legislations derived from an agreement aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP" (a component of the "ACP-Information and Communication Technologies Programme" within the framework of the 9th European Development Fund). These projects are primarily aimed at political, social, economic and environmental development, market integration, and investment facilitation in the area through harmonisation and improvement of the information and communication technology and connectivity. However, both the ITU and EU have a keen interest in stimulating cybercrime regulation in the region. The fight against cybercrime may not be a priority for developing countries since they do not (yet?) rely as heavily as the western world on information technologies. Flaws in cybercrime legislation tend to make these regions safe havens for hackers: hence the interest from the western countries to stimulate the implementation of cybercrime provisions.

I.III.II. TREATIES ON CYBERCRIME.

Presently, no purely international treaty on cybercrime exists. The adoption of a comprehensive international convention has mainly been frustrated by different sensibilities on the scope of criminalisation – such as the balance between freedom of expression and criminalisation of hate crimes – diverse reliance on technology in developed and developing countries, and problems related to political distrust between States and the intrusiveness of extraterritorial investigation tools.[79] At the international level, the sole binding instrument that contains provisions on cybercrime is the Optional Protocol to the United Nations Convention on the Rights of the Child, on the Sale of Children, Child Prostitution and Child Pornography (2000). The provisions therein are exclusively related to child pornography.

Conversely, due to a higher level of political, technological, and legal homogeneity, several binding instruments have been adopted at regional levels: the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information (2001), the substantive scope of which is aimed at providing harmonisation of provisions concerning the illegal accessing of computer systems and data, and the creation, use, or distribution of malicious software; the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009), which covers information warfare, cyber terrorism, and threats to national and international information systems and critical infrastructures; the League of Arab States Convention on Combating Information Technology Offences (2010)[80], which in its substantive scope includes offences of cyber terrorism, organised crime committed by means of information technology, and reference to an aggravating circumstance of committing traditional crimes by means of information technology; finally, the African Union Convention on Cyber Security and Personal Data Protection (2014), which adopted a broader approach to the issue of cyberlaw, covering cybercrime, electronic transactions, cybersecurity, data protection, and privacy.

The European area was notably prolific. In 2001, a Convention on Cybercrime was adopted under the aegis of the Council of Europe (CoE). The convention, known as the "Budapest Convention", remains the most critical instrument on cybercrime, and the only instrument with a "quasi-

---

[79] See also M. Gercke, 'Hard and Soft Law Options in Response to Cybercrime' (n 66) 187, 197. See also Chapter 4 – Jurisdiction and International Cooperation.

[80] See also Economic Community of West African States, *(Draft) Directive on Fighting Cybercrime* (2009); African Union, (Draft) Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012).

international" reach.[81] Furthermore, within the European Union, two instruments have addressed cybercrime: Framework Decision 2005/222/JHA on Attacks against Information Systems,[82] aimed at stimulating harmonisation on Member States' provisions concerning cyberattacks, and its repealing Directive, 2013/40/EU[83].

I.III.III. THE COE CONVENTION ON CYBERCRIME.

The CoE Convention on Cybercrime, together with its Additional Protocol[84], represents the most important cybercrime convention due to its number of ratifications, its geographical diffusion, and the potential scope of its application. It followed a long preparation process, which took four years of negotiations and twenty-seven drafts.[85]

Essentially, the CoE Convention adopts a holistic approach to cybercrime. It requires its States-parties to introduce criminal offences and sanctions for four basic categories of computer crimes into their substantive penal law.[86] It mandates the adoption of procedural law tools aimed at detecting and investigating computer crimes, with particular attention given to the collection and preservation of electronic evidence.[87] Specific consideration is further devoted to the establishment of a rapid and efficient system of international cooperation.[88] Finally, the Convention requires that member States adhere to an adequate standard of human right protection in the fight against cybercrime.[89]

---

[81] CoE, *Convention on Cybercrime,* ETS 185, 23 November 2001. The CoE Convention is open for signature by "non-member States which have participated in its elaboration" (CoE Cybercrime Convention, Art. 36.1). As of today, several non-member States (such as Canada, Japan, South Africa and the United States of America) have signed the Convention.

[82] EU, *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, OJ L 69, 16.3.2005.

[83] EU, *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, OJ L 218, 14.8.2013

[84] CoE, *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, ETS 189, 28 January 2003..

[85] See CoE, *Explanatory Report to the Convention on Cybercrime*, ETS 185, 23 November 2001, Part II.

[86] See *infra* Chapter 2 – Substantive Law.

[87] See *infra* Chapter 3 – Procedural Law.

[88] See *infra* Chapter 4 – Jurisdiction and International Cooperation.

[89] …including "rights arising pursuant to obligations (the State-party) has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality" CoE, *Convention on Cybercrime* (n 81), Article 15.1.

Indisputably, the CoE Convention on Cybercrime has proved and continues to prove to be a useful tool in the fight against cybercrime, due to its comprehensive approach and its "technology-neutral" terminology.[90] Its global success demonstrates its importance. It is used as the primary model in national and international legislation on cybercrime,[91] and it has an international reach that extends far beyond the borders of Europe. As of today, the CoE Convention on Cybercrime has been ratified or acceded to by 64 States, including 20 non-Members of the Council of Europe, such as Australia, Canada, Japan, and the United States of America.[92]

There is a strong determination to enhance the international reach of the Budapest Convention. In November 2010, a working group on cybercrime and cybersecurity was jointly established by the United States and the European Union with the task, *inter alia*, of assisting non-European states to become parties to the Convention.[93] Its imitation and diffusion have been supported by the Council of Europe Global Project on Cybercrime, the aim of which was to promote the broad implementation of the Convention on Cybercrime, along with its Protocol on Xenophobia and Racism, and to deliver specific results in terms of legislation, criminal justice capacities and international cooperation.[94] In 2010, the United Nations General Assembly recommended the use of the CoE Convention as a "litmus test" for the development of the "necessary legislation for the investigation and prosecution of cybercrime"[95]. Its international reach and ambition induced many commentators to consider the CoE Convention as the first and only binding "international" treaty on cybercrime.[96]

---

90 See A. Seger, 'The Budapest Convention 10 Years in: Lessons Learnt', in S. Manacorda (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 170.

91 See also: A. Seger, 'The Budapest Convention 10 Years in: Lessons Learnt' (n 90), 168-169.

92 See CoE, *Convention on Cybercrime, Chart of signatures and ratifications* <www.conventions.coe.int>. According to CoE, *Convention on Cybercrime* (n 81), Article 37: "the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention".

93 See S. Schjolberg, 'Potential New Global Legal Mechanisms on Combating Cybercrime and Global Cyberattacks', in S. Manacorda (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012), 180-181.

94 See CoE, *Project on Cybercrime Final Report*, ECD-567(2009)1, 15 June 2009.

95 UN GA, *Resolution 64/2011, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical infrastructures*, 17 March 2010, A/RES/64/211.

96 See, *inter alia*, B. Harley, 'A global convention on cybercrime?' (2010) Columbia Science and Technology Law Review 11; S. Schjolberg and S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime* (AitoOslo 2011). According to Gercke, "Although the Convention on Cybercrime is supported by various international organizations, the fact that ten years after it has been opened for signature the United States is the only non-European country that has ratified the Convention underlines its de jure status as a regional vis-à-vis international instrument" (M. Gercke, 'Hard and Soft Law Options in Response to Cybercrime' (n 66), 196). Supposedly, the numerous ratifications that happened after 2010 may be deemed to have "nullified" Gercke's argumentation.

Nevertheless, the Convention has been criticised for its supposed "western-centrism". Having been drafted by and for western States, the Convention may be considered a predominantly European (*rectius*: western) instrument, expressing points of view that may not be globally accepted.[97] However, the Convention's main drawbacks are structural. It entered into force in 2001, after four years of negotiations. It was thus discussed and formulated in the late 1990s. The Convention may therefore be deemed to have an archaic and obsolete approach to cybercrime. In two decades, technology has undergone drastic changes, and so has cybercrime. It may be contested that the Convention is still able to adequately address cybercrime investigation, prosecution, interstate cooperation, and human rights protection.

[97] See M. Watney, 'Cybercrime Regulation at a Cross-Road: State and Transnational Laws Versus Global Laws', in *International Conference on Information Society* (IEEE 2012), 73.

I.IV. PROBLEMS AND CHALLENGES OF THE EXISTING FRAMEWORK.

The fight against cybercrime strictly depends upon the existence of a coherent, internationally coordinated response, based on a harmonised substantial framework and the existence of procedural and cooperation tools suited to the peculiarities of this crime. As pointed out by the CoE Convention Explanatory Report: "(t)he new technologies challenge existing legal concepts. (…) Solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments"[98].

Several multilateral instruments have been adopted to stimulate a common regulation of cybercrime and the diffusion of *intra* and *extra moenia* investigative procedures, apt for dealing with electronic data. Generally, such instruments have addressed how digital technologies have impacted on crime and its traces.

Technology (like its social reverberations) is continuously evolving. As it evolves, its modifications affect crime and the methods for dealing with data. This process of evolution may require an almost constant revision of the law, imposing an "expiry date" on legislation. As a consequence, it may particularly jeopardise the efficiency of an international convention on cybercrime, which is more difficult to amend than national statutes.

The multilateral treaties on cybercrime implemented the use of technology-neutral terminology to avoid accelerated ageing. This solution was perilous, as it sacrificed precision for efficiency. At a substantial level, this approach implied "one size fits all" provisions, which are unable to delineate the target behaviour in detail. It also fostered the idea that a simplistic and generalised thinking about technology (e.g. perceiving "computer systems" as comprising every type of electronic device) was sufficient.

Higher precision in defining the scope of provisions was thus entrusted to domestic implementation. This naturally created discrepancy between the systems involved and decreased harmonisation. Moreover, it left the perimeter of the norm (in particular, the limits to excessive criminalisation) to be set at the domestic level, through its general principles of criminal law and the applicable human rights provisions.

---

[98] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 6.

The balancing process between the international obligation, human rights, and general principles of criminal law was not considered in the major cybercrime instruments. Nevertheless, these principles and rights are often affected by new technology. Rights to digital privacy, expression, or assembly may not be sufficiently protected by their traditional formulation.

The inability to provide a holistic approach to cybercrime – comprising principles and rights involved – is one of the most significant flaws that recurs in the multilateral cybercrime instruments.

These instruments have also been affected by a general lack of understanding and precise selection of the targeted technology / conduct. Important issues (e.g cryptography, or Denial of Service attacks[99]) were left unanswered. Many provisions were constructed by tracing their analogous, non-digital "twin" provision – as they were new technological forms of the same crime or the same procedural power.

In particular, multilateral cybercrime instruments seemed unable to grasp the anthropological impact of new technologies. The cyber realm is governed by different rules than those on which criminal law is founded. Among them, the behaviour of its users may respond to different psychological and sociological stimuli than the "man on the Clapham omnibus".

The Internet is now central to the lives of most people. It is the place where many persons conduct a large proportion of their everyday activities, from buying services or goods to chatting with friends. In this virtual agora, the user may behave according to different rules than the person on the bus. This difference also exists when he or she is committing a crime.

Furthermore, this digital agora is international, and necessitates internationally agreed and harmonised rules that deal with its spatial conception. Every day, the Internet user sends and receives data to and from all over the world. He/she continually crosses invisible borders. However, the user's perception and expectation of jurisdiction over his/her acts are different from that of a citizen acting in the "real world". The user looks to both the Information Technology Company (ITC)[100]and the State of citizenship or residence (most of the time in a mutually exclusive way) for protection against other malevolent users or abusive actions by States (both the State of citizenship or residence, and other States potentially acting online). The actors in the international digital system are changing and the legal framework around cybercrime must address this change.

---

[99] A Denial of Service attack is a type of cyberattack aimed at interrupting or suspending the availability of a computer system or network. The most common type of DoS attack is conducted by saturating the target system with requests (e.g. by conducting numerous coordinated over-usage of legitimate services on a website), which lead to a server overload. Some applications (such as "Floodnet") can be used to generate automated Denial of Service. A DDOS (Distributed Denial of Service) is a Denial of Service attack conducted by multiple systems at once, usually through the use of botnets.

[100] An Information Technology Company (or Tech Company) is a type of business entity that offers electronics-based technology products or services, including Internet-related services such as social networking services.

The multilateral instruments on cybercrime have had a great deal of success in creating a harmonised substantial framework and diffusing procedural and cooperation tools suited to new technology. Most States have introduced legislation on cybercrime under their stimuli. However, at the beginning of the third decade of the third millennium, this framework is in danger of crumbling.

Old technologies are changing, and new technologies are emerging. Most of the resulting social implications are revolutionary. The existing cybercrime international framework struggles to cover this evolution, and numerous areas remain unregulated.

States are often left with no guidelines, relying on autonomous decisions, which – applied in cyberspace – may have international consequences. It is a matter of concern that such solutions frequently imply an overextension of the State *ius puniendi*, in defiance of the basic human rights of the suspect / accused.

How can a framework conceived twenty years ago, burdened by atavistic problems, face the incipient fourth industrial revolution, where new disruptive technologies, such as artificial intelligence, are drastically changing world society?

These past solutions, present problems, and future challenges will be the focus of this work.

This dissertation will undertake an analysis of the main multilateral instruments on cybercrime and their domestic implementation, with the aim to discover whether these instruments have succeeded in creating a coherent response to cybercrime. It will highlight how obligations under that legislation currently interacts both with the primary human rights of the suspect / accused, and with the evolving technological panorama. It will reflect on the ability of the cybercrime legislation to cope with future legal and technological challenges. It will offer recommendations for improvement at the normative and interpretative level, devoting particular attention to a more beneficial relation between criminalisation and human rights protection.

Three main areas will be evaluated: substantive law[101], procedural law, and international cooperation and jurisdiction. The chapters herein will follow the structure of the multilateral instruments, adopting a top-down approach (from the international to the national level). Due to its importance, the CoE Convention will be the normative pillar of this work. Particular consideration will also be devoted to the EU instruments on cyberattacks.

The European experience represents the most exciting example of harmonisation at the substantive, procedural, and cooperation level, due to its unique intersection of important cyber-specific and

---

[101] From a substantive point of view, this work will focus on the core cybercrime offences - i.e. offences against the confidentiality, integrity and availability of computer data and systems. Other types of cybercrimes *lato sensu*, such as content or copyright-related offences, will not be considered.

human rights instruments. Although it will not engage in a systematic comparative study, this paper will analyse the most prominent European systems,[102] in order to highlight the legislative and judiciary solutions better suited to exemplify its normative assumptions. Where relevant or necessary to the analysis conducted, legal systems outside the European area will be considered, with particular attention given to the American experience.

[102] Also due to language limitations of the author.

II SUBSTANTIVE LAW

"There are only 10 types of people in the world: those who understand binary and those who don't."[103]

[103] Famous mathematical joke, author unknown.

II.I. INTRODUCTION.

Cybercrime is a broad legal concept, its meaning not being wholly precise and stable. Today, no common legal definition of cybercrime exists. In general terms, cybercrime comprises illegal conduct against or with the use of digital technology. It includes a wide range of crimes involving technology to varying degrees.[104] Among the various types of "computer-related"[105] offences, there is a group of offences designed to directly protect data and computer systems against external attacks aimed at compromising their confidentiality, integrity, or availability. These offences are commonly considered to be cybercrime *stricto sensu.*

This chapter focuses on cyberattacks, which is to say on the cyber offences related to the confidentiality, integrity, and availability of computer data and systems. It considers the evolution, within the domestic criminal systems, of the basic cyber-specific substantive structure. In particular, it highlights the role of the main multilateral cybercrime instruments in the construction of a "minimum" level of substantive legal protection for computer systems and data. It is asserted, however, that the construction of this minimum standards was substantially affected by a series of issues which were not sufficiently considered at the international level, namely: the influence of the general principles of criminal law on the criminalisation obligation, once inserted in the domestic criminal system; the lack of a precise definition of the legal interest protected by the norm; the use of vague and technologically-neutral terminology; a lack of attention paid to the problems related to the *maximum* criminalisation and specifically to the principle of proportionality between criminal offences and penalties, and the *ultima ratio* and *lex certa* principles.

Particular attention is paid in this chapter to Denial of Service (DoS) attacks (i.e. attacks aimed at saturating the target machine with external communications requests in order to impede its functioning). DoS attacks are among the most common types of cyberattack, and present strong analogies with the typical street rally. They are often used as an "electronic" form of protest, aimed at blocking access to a digital space with the concurrent presence of protesters. The analysis of DoS attacks therefore tends to consider whether it is possible to delimitate a legal space in which cyber protest conducted through DoS attacks may take place, wherein protesters' rights are protected by standards of freedom of expression and assembly.

---

[104] See C. Ram, 'Cybercrime', in N. Boister and R. J. Currie (Eds), *Routledge Handbook of Transnational Criminal Law* (Routledge 2014), 379.

[105] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 18.

Furthermore, this chapter takes into consideration the specific issues related to large-scale cyberattacks. These cyberattacks target the availability and functioning of the State's critical infrastructures, and harm or endanger essential national and international legal interests. This chapter reflects on the propensity of a supranational extension of the legal interests affected by socio-technological evolution and the increasingly transnational nature of digital infrastructures. Consequently, it contemplates the increasing role of the international system within the substantive protection of these interests. Furthermore, this chapter considers the way large scale cyberattacks are legally qualified. In particular, it analyses situations where – on the basis of their scale and effect, and the meeting of the required material and mental elements of the offence – such attacks can be labelled as terrorism.

Finally, this chapter analyses the application of traditional models of collective crime to the conduct of cyberspace-based criminal groups. Today, most cyberattacks, in particular those that take place on a large scale, are conducted by organised hacker groups. Alongside the predicated cyber offences, such groups may thus be charged with joint crime offences such as conspiracy or crime of association. However, the legal framework on these latter offences does not sufficiently take into consideration the specific characteristics of digital organisations. Through a case study (i.e. the hacker collective "Anonymous") this chapter considers how common-law conspiracy doctrines and civil-law criminal association models are applied to digital crime. The legal analysis herein is combined with socio-criminological findings which reveal the operational and morphological characteristics of organised cybercrime.

II.II. HARMONISATION OF CYBERCRIME LAW: SOME PRELIMINARY CONSIDERATIONS.

In their 1988 analysis on the regulation of cybercrime, Hollinger and Lanza-Kaduce noted that "scholars are rarely afforded contemporary opportunities to study the formation of criminal law".[106] Cybercrime is undoubtedly one of these rare opportunities. In a relatively short period of time, the emergence and diffusion of new technologies have induced new criminal behaviours, which in turn have led to the adoption of a new set of criminal offences.

Due to the transnational character of cybercrime, the creation of a cybercrime legislation has been intensely stimulated at the international level. A particular amount of stimulation has been exerted within the European region by a significant intersection of cybercrime instruments. In 1989, the Selected Committee of Experts on Computer-related Crime, appointed in 1985 by the CoE European Committee on Crime Problems, drafted a Recommendation and an accompanying Report on Computer-related Crime[107] containing a minimum list of cyber offences whose introduction was recommended to States.

In 2001 the CoE Convention on Cybercrime was adopted. The treaty was drafted by a committee of experts, set up by the European Committee on Crime Problems. The Committee considered that "whilst Recommendation No. (89) 9 resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena."[108] From the "minimum consensus, not excluding extensions in domestic law"[109] underlying the treaty, originated a list of offences whose inclusion in the domestic systems of the State Parties was reciprocally obligated. The 2001 CoE Convention on Cybercrime, due to its geographical scope and its comprehensive approach, rapidly became the most important multilateral instrument on cybercrime. [110]

---

[106] R. C. Hollinger and L. Lanza–Kaduce, 'The process of criminalization: The case of computer crime laws' (1988) 26 Criminology, 101, 101.

[107] CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 9.

[108] CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), at §9.

[109] CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), at §34.

[110] See *supra* § I.III.III.

The European Union was geographically covered by the Convention on Cybercrime, and its member States signed it on the very day of its opening, with some minor exceptions.[111] However, one year after the adoption of this comprehensive treaty, the European Commission proposed the adoption of a Framework Decision aimed at an approximation of criminal law in the area of attacks against information systems. The proposed instrument was substantially overlapping *ratione loci et materiae* with (a part of) the CoE Convention. The Commission acknowledged the intersection with the CoE Convention. It stated that the proposed Framework Decision was "intended to be consistent with the approach adopted in the Council of Europe Convention for these offences".[112]

In 2005, the Council of the European Union adopted the Framework Decision 2005/222/JHA on attacks against information systems. In 2013, the Framework Decision has been replaced by Directive 2013/40/EU, chiefly to address the shortcomings of the former with regards to large-scale cyberattacks.

Due to its sophisticated normative system, the European legal framework is of particular interest in the study of cybercrime. In the European area, a stratification of four instruments on cybercrime has uniquely shaped the set of cybercrime offences. An attentive analysis of existing domestic norms reveals the passage of such instruments and the imprint they have had on the national normative systems.

However, before embarking on a normative analysis of the main cybercrime offences, it is important to briefly set forth a series of preliminary considerations, which may help to better appraise the various factors that contributed to the creation of the cybercrime substantive framework, shaped its current form, and may guide its future evolution.

II.II.I. FEAR OF THE CYBER-DARK: A POTENTIAL FOR OVERREACTION.

Indisputably, the pivotal factor that induced the enactment of a cybercrime framework was the inefficiency of traditional criminal offences to cover new technology-related criminal behaviours. For instance, the main British computer hacking Statute – the Computer Misuse Act – was enacted in 1990, in response to concerns about the inefficacy of the existing legislation to adequately

---

111 See CoE, *Convention on Cybercrime, Chart of signatures and ratifications* (n 92).

112 EU, *Proposal for a Council Framework Decision on attacks against information systems*, COM(2002)173 final, OJ C 203E , 27.8.2002, 8.

regulate computer hacking. These glitches are perfectly illustrated by the 1988 case of *R v Gold and Schifreen.*[113] The case involved the hacking of the British Telecom computer network. The defendants were charged with forgery under the UK[114] Forgery and Counterfeiting Act 1981. The Court of Appeal and, subsequently, the House of Lords, acquitted the defendants. The reasoning behind these decisions was based on the impossibility of subsuming "electric impulses" under the language of the Act. According to the House of Lords, the "attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated."[115]

The kinds of operational malfunctions experienced in the application of traditional offences to digital criminal phenomena required the enactment of new offences tailored to cover cybercrime.

To the extent that a parallelism between digital offences and their physical equivalents is possible (as will be considered further in subsequent subchapters), the scale of punishment for the new offences was substantially higher than for their traditional counterparts. Consider for example criminal trespass, which was one of the offences applied to illegal access to computer systems and data, in the absence of a specific cyber offence.[116] Criminal trespass is usually considered a misdemeanour. In the UK, according to the UK Criminal Justice and Public Order Act 1994, section 68, aggravated criminal trespass[117] is punished with imprisonment for a term not exceeding three months, or a fine, or both. Under the UK Computer Misuse Act, illegal access to a computer system could be punished with imprisonment for a term not exceeding two years, or a fine, or both.[118]

This begs the question: what are the reasons for such a disparity in sanctions? The primary reason could be related to the typical vulnerability of data, and to the highly sensitive information that they may contain. A subsequent question may be: are the contents in a computer system to be valued so much more than what is protected in a physical domicile? Interestingly, this question is central to cybercrime law, as it is the analogy between physical domicile and digital devices.

---

[113] UK, *R v Gold and Schifreen* [1988] AC 1063, HL, [1987] 1 QB 1116, CA. See, generally, on the 1990 Computer Misuse Act, M. Wasik, 'The Computer Misuse Act 1990', (1990) Criminal Law Review 767; N. F. MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 Criminal Law Review 955.

[114] In this work, UK is generically used for acts that may have a geographical extent over England, Wales, Scotland and/or Northern Ireland.

[115] UK, *R v Gold and Schifreen* [1988] AC 1063 at 1069, HL.

[116] See *infra* § II.III.I.

[117] With the intent of intimidating persons engaging in a lawful activity so as to deter them or any of them from engaging in that activity, of obstructing that activity, or of disrupting that activity.

[118] UK, *1990 Computer Misuse Act*, Section 1: "A person guilty of an offence under this section shall be liable: (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both".

In particular during the early criminalisation of cybercrime, where digital technologies did not have the same diffusion and relevance of today, spurious elements may have influenced the scope of the new legislation. In particular, notwithstanding a scarce empirical corroboration, a rising apprehension for possible cyberattacks against essential digitalised social and political interests was of particular relevance within the formation of cyber law. Fear – as an irrational and exceptional reaction of the mind that induces an abrupt change in the normal metabolic functions of the body – can greatly affect the fundamental tenets of criminal law.[119] It may influence the relation between the actual interest in protecting a legal value and criminal punishment, leading to disproportionate sanctions.

This anxiety – epitomised concerns such as the fear of terrorist or military cyberattacks "against the dam"[120] – partly rests on the difficulties of understanding the phenomenon of cybercrime, which is often hidden beneath a complex mathematical code, but at the same time is immanent in daily life ("too many digital wolves could blow down my digital piggy-house!"). Partly, this anxiety is based on the influence of media and science fiction, which have explored the development of and the risks related to digital technology (even including related legal issues, such as Asimov's famous "laws of robotics") and have filled the gap of our inability to understand the problem (with facts lacking empirical consistency).[121]

Particularly in the initial phase of criminalisation, media had a direct and significant effect on the extent of legislation.[122] Newspapers gave extensive coverage to cyber incidents, such as the attacks of the hacker group "the 414s".[123] In 1983, the blockbuster movie "Wargames" had a critical impact on public opinion, profiling hackers and depicting them as able to break into military digital

---

[119] On the relation between emotions and criminal policy see: S. Karstedt, I. Loader and H. Strang, *Emotions, crime and justice*(Hart 2011); F. E. Zimring and D. T. Johnson, 'Public opinion and the governance of punishment in democratic political systems', in *The Annals of the American Academy of Political and Social Science* (2006), 265–280.

[120] See for instance: D. Usborne, 'Bowman Avenue Dam: US in fear of new cyber attack as dam breach by Iranian hackers is revealed' (The Independent 21 December 2015) <http://www.independent.co.uk/news/world/americas/bowman-avenue-dam-us-in-fear-of-new-cyber-attack-as-dam-breach-by-iranian-hackers-is-revealed-a6782081.html>: "The hackers got into its control system, potentially allowing them to release larger volumes of upstream water without warning, through a cellular modem". In all probability the attackers merely gained access to some back office systems (See: D. Volz and N. Raymond, 'U.S. to blame Iran for cyber attack on small NY dam' (Reuters 10 March 2016) <http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WC2NH>).

[121] See e.g. *supra* n 16.

[122] See R. C. Hollinger and L. Lanza–Kaduce, 'The process of criminalization: The case of computer crime laws' (n 106), 105.

[123] See J. Kirchner, 'Hackers steal legislators' attention' (ComputerWorld 12 September 1983) <http://www.computerworld.com/article/2523544/government-it/hackers-steal-legislators--attention.html>.

infrastructure and set off war.[124] The press began to write more about hacking and hacker nuisances,[125] occasionally exaggerating data on attacks.[126]

It seemed that such extra-legal factors – providing for an approximate or fictitious sketch of the criminological phenomenon of cybercrime – combined to create the necessary backdrop for the enactment of the main US computer hacking legislation: the 1986 US Computer Fraud and Abuse act. The movie "Wargames" was shown and repeatedly mentioned during the drafting in the House Committee on Science and Technology.[127] The committee's chairman considered that the movie "outlines the problem fairly clearly", illustrates "certain break-in methods that are factual"[128], and "is quite realistic in terms of what real hackers do"[129]. It even called to "prevent these 'Wargames' types of break-in in the future".[130] Unsurprisingly, the validation of Wargames as depicting a real problem was backed by computer industry representatives.[131] A policy maker is not a technician: in order to understand technical issues, the help of an "expert" is needed. *Ça va sans dire*, however, that if the expert is a stake-holder or a potential victim, they may tend to exaggerate or underplay the scenario, encouraging the legislator towards a favourable normative framework.

This "fear-factor" was gradually absorbed into the national and international political discourse. For instance, even before the massive cyberattack that struck Estonia in 2007[132], the European legislator noted the "increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States"[133]. A factual concern that has remained "potential" until now, since no "terrorist attacks against information systems" have ever happened. However, such concerns infiltrated the media, with an unrestrained use of the words "cyberwar" and "cyberterrorism"[134], and the scholars, with a massive increase in work on these topics. Furthermore, such concerns affected the international and national legislators, with concrete

---

[124] See M. Mitchell and N. Mitchell, '5 Amazing Ways WARGAMES Changed the World' (TheGeek Twins, 6 April 2014) <http://www.thegeektwins.com/2014/06/5-amazing-ways-wargames-changed-world.html#.Vurr5bReSng>. See also S. Ricker Schulte, *Cached: Decoding the Internet in Global Popular Culture* (NYU Press 2013), Chapter 1 "The 'Wargames Scenario': Regulating Teenagers and Teenaged Technology".

[125] See R. C. Hollinger and L. Lanza–Kaduce, 'The process of criminalization: The case of computer crime laws' (n 106), 107.

[126] See J. K. Taber, 'A survey of computer crime studies.' (1980) 2 Computer Law Journal 275, 310.

[127] US, *Computer and Communications Security and Privacy: Hearings Before the Subcommittee on Transportation, Aviation, and Materials of the Committee on Science and Technology*, U.S. House of Representatives, Ninety-eighth Congress, First Session (1983), 24.

[128] *Id.,* 1.

[129] *Id.,* 13.

[130] *Id.,* 4.

[131] *Ibid*. See also S. Ricker Schulte, *Cached: Decoding the Internet in Global Popular Culture* (n 124) 48-9.

[132] See *infra* § II.VI.III, n 404ff.

[133] EU, *2005 Framework Decision on attacks against information systems* (n. 82), Preamble.

[134] See *infra*, n 405.

repercussions over the criminal provisions to be applied on cybercrime. While it is perfectly reasonable to stress that "those who fail to anticipate the future are in for a rude shock when it arrives"[135], criminal punishment ought not be based on a fearful anticipation.

II.II.II. TECHNOLOGY AS AN ELEMENT OF THE CRIME, AND THE USE OF TECHNOLOGY-NEUTRAL TERMINOLOGY.

Cybercrimes are technology-related criminal behaviours. Digital technology is an element of the crime, and a central component of its definition. However, using a technological precise definition may lead the provision to "expire" when technology evolves, requiring its constant revision. Most multilateral instruments on cybercrime employed technology-neutral language, in order to afford the provisions therein a broad scope of application on present and future technologies.[136]

An interesting depiction of the problems relating to technology-neutral (or independent) or technology-oriented (or dependent) legislation is to be found in the 1998 Dutch policy memorandum "Legislation for the Electronic Highways", which states that: "Technology-independent legislation is to be preferred. This usually establishes an equality between the 'off-line world' and the 'on-line world'. Also, technology-independent legislation can better withstand technological turbulence. However, sometimes technology-dependency will be called for instead. For instance, the need for legal certainty could be a reason for technology-dependent legislation."[137]

The memorandum perfectly illustrates the problems underlying the use of technology oriented or neutral language. First, the use of technology-neutral language relates to the need for a cybercrime provision to be applied on the broadest range of technologies used for or targeted by a crime. It overcomes the "rigidity" of the law, whose rate of reform may not be sufficient to follow technological evolution. Second, technology-neutral legislation mainly focuses on the "non-technological" part of the act. It emphasises the similarities between cybercrimes and physical (traditional) crimes (e.g. illegal access to computer systems is "similar" to criminal trespass; data interference is "similar" to criminal damage). Consequently, it reduces the need for a metaphysical abstraction by the legislator and the interpreter in the analysis of cybercrime, and allows analogy

---

[135] R. Smith, P. Grabosky and G. Urbas, *Cyber criminals on trial* (CUP 2004), 156 – apparently, one of the most quoted phrases on cybercrime.

[136] See, for instance, CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §36.

[137] As reported, and translated from Dutch, in B. Koops, 'Should ICT regulation be technology-neutral?' in B. Koops, M. Lips, C. Prins and M. Schellekens, *Starting points for ICT regulation. Deconstructing prevalent policy one-liners* (Asser Press 2006), 77.

with existing and "well rooted" criminal behaviours.[138] Third, the balance between broader neutral formulations and narrower oriented terminology is to be found in the principles of certainty and foreseeability of criminal law.[139] The need for avoiding excessive rigidity of the law and to keep pace with evolving technology should be balanced against the right of the individual to understand from the definition of the offence (possibly with the aid of judicial interpretations) what acts or omissions are prohibited. [140]

In most cases, however, the balance has tended towards the need for flexible legislation. [141]

With regard to the international cybercrime instruments, the use of technology-neutral formulations does not conflict with the principles of certainty and foreseeability, due to the lack of direct enforceability of the international norm. Moreover, any international instrument, being more difficult to amend than national laws, is more resistant to modification, and may therefore require a higher level of "neutrality" in the technological definitions it employs. Eventually, the domestic system is the appropriate forum in which to analyse the scope of technology-neutral terminology and confront it with the aforementioned principles.[142]

Nevertheless, the formulation of international provisions in abstract terms may have repercussions on the consistency of their internal transposition.[143] Technology plays a pivotal role within the cyber offence and constitutes its necessary material element. Ambiguous wording and vague terminology leave ample space for internally implementing an international obligation. Eventually, it may lead to substantially dissimilar domestic provisions.

---

[138] It should be stressed again, however, that such an "analogical" approach may hinder a correct appraisal of digital behaviour.

[139] See B. Koops, 'Should ICT regulation be technology-neutral?' (n 152): "regulation should be as much technology-neutral as is compatible with sufficient legal certainty".

[140] See, *inter alia*, ECtHR, *Kokkinakis v Greece* (Application no. 14307/88) 25 May 1993, § 52 "… an offence must be clearly defined in law. This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable."

[141] See, *inter alia*, ECtHR, *Cantoni v. France* (Application no. 17862/91) 15 November 1996, § 31: "As the Court has already had occasion to note, it is a logical consequence of the principle that laws must be of general application that the wording of statutes is not always precise. One of the standard techniques of regulation by rules is to use general categorisations as opposed to exhaustive lists. The need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. The interpretation and application of such enactments depend on practice."

[142] See, *ex plurimis*, US, *United States v. Mitra* 405 F.3d492 (7th Cir.2005); GER, *Strafgesetzbuch* Section 263; M. Gercke and P. W. Brunst, *Praxishandbuch Internetstrafrecht* (W. Kohlhammer Verlag 2009), 101.

[143] Cf, CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 29 "Although preciseness is important in the wording, the offences should not be so technologically oriented that the new provision ceases to be effective in the near future when the same abuse is done by somewhat different means as a result of technological development".

II.II.III. INTERACTION BETWEEN THE INTERNATIONAL OBLIGATION AND THE DOMESTIC SYSTEM.

National systems represent the first and most important level of the criminal repression of cybercrime. Aside from cases where a cyberattack is qualified as a "common" international crime (e.g. as a war crime), there is currently no international cyber-specific offence. However, the influence of multilateral instruments has been of pivotal importance in shaping the scope of the domestic cybercrime provisions. Only in sporadic cases have domestic cybercrime offences been enacted before any intervention at the international level.[144]

The interaction between the international and domestic levels, however, is somewhat tortuous. Notwithstanding the large role played by the international instruments in stimulating the harmonisation of cybercrime law, the analysis of the existing substantive legal framework reveals a certain lack of coherence.

The international harmonisation of criminal law is grounded on States' common interest in the transnational repression of crimes.[145] Harmonisation is carried out through the insertion of a normative core – which is the object of the international obligation – within the domestic legal system (if, and to the extent to which it is absent). Such incorporation is far from being aseptic. The encircling normative system contaminates the transplanted norm and influences its nature. The very position of the norm within the code may affect its construction, interpretation, and evolution. Concepts and interpretations developed with regard to surrounding provisions may be applied on the new offences – in particular, where analogical linkages between them are acknowledged. This is particularly true with regard to cybercrime.

---

[144] Key examples of this are the US and FR systems (FR, *Loi n. 88-19 du janvier 1988 relative à la fraude informatique*). See inter alia: H. Croze, 'L'apport du droit pénal à la théorie générale de l'informatique (à propos de la loi n 88-19 du 5 janvier 1988 relative à la fraude informatique)', (1988) 18 La Semaine Juridique Edition Générale (1988). In most systems the first introduction of a set of cyber offences was encouraged by the multilateral instruments on cybercrime (for instance, ITA, *Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"* – see, *inter alia*, S. Resta, 'Informatica, telematica e computer crimes' (1997) 6 Informatica e diritto 143.

[145] Traditionally, the *ius puniendi* is a sovereign prerogative of the State. More than other branches of law, criminal law tends to muscularly resist to legal harmonization, even if focused on the transplant of a "minimum". See A Klip and H Van der Wilt (eds), Harmonisation and harmonising measures in criminal law (Royal Dutch Academy of Sciences 2002); U. Sieber, 'The Forces Behind the Harmonization of Criminal Law', in Mireille Delmas-Marty (ed), *Les chemins de l'harmonisation pénale, Harmonising criminal law* (Société de Législation Comparée, 2008), 386.

In creating a cybercrime substantive framework, most systems have matched cyber offences to the traditional offences to which they seemed analogically close.[146] This solution was not intended to create any explicit relation between the "physical" common offence and the cyber offence. However, it produced a form of dependence between them, in terms of both the legislative formulation and the legal interests protected; almost as if the new offences represented new forms of impingement upon the traditional legal interests protected by the criminal system.[147] This "analogical rationalisation" may influence the cyber offence's interpreter, who may be tempted to view it through the lenses reserved for the traditional norm (and its gravitating system of theoretical and jurisprudential production).

Traditional criminal law concepts are constructed in order to depict physical behaviours and the related scientific rules governing them. They may be unable to successfully cover the characteristics of cybercrime, which are related to the role of digital technology within the offence.

A novel approach may be needed. For instance, this approach can be provided by giving to cybercrime law a "sterile lab" within the legal system, protected from external contamination. Few systems placed the cyber offences in new specific titles within the code (e.g. the Belgian system)[148] or enacted special legislation on cybercrime (e.g. the Portuguese system)[149].

A further issue relates to the influence of the general part of criminal law on the cyber offence. Most criminal systems are composed of a "special part", which contains and rationalises the concrete offences, and a "general part", which expresses the background criminal policies of a State and its general doctrines related to criminal liability.[150] The general and special part of the criminal code are intrinsically interrelated. In particular, the scope of application of an offence is largely influenced by the general principles at work within a given system. For instance, a proposed norm may indicate its required mental element, or how preliminary conducts should activate liability. Yet, their exact meaning is dictated by the concepts of intention or attempt present in the general part or

---

146 See, for instance, the Italian system: ITA, *Camera dei Deputati, XI Legislatura, Disegno di legge n. 2733, Presentazione del Ministro di Grazia e Giustizia G. Conso*; I. Salvadori, 'L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica', in L. Picotti (ed.), *Tutela penale della persona e nuove tecnologie* (CEDAM 2013).

147 *Id.,* 130ff.

148 See *infra* n 196.

149 See Portugal, *Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime)* – which pays a strong structural dependence to the CoE Convention and EU 2005 Framework Decision.

150 This classification is typical of the Romano-Germanic tradition.

elaborated by case-law or doctrine. [151] On these general principles States continue to maintain an absolute prerogative, and no serious harmonisation attempt has been made.[152] However, as it will be discussed in the following normative analysis, national differences on these principles may greatly vary the scope of an internationally induced offence.

Traditionally, the multilateral criminal treaties are substantively aimed at setting a common standard of criminalisation in relation to what to punish.[153] These treaties tend to stimulate either the introduction of a criminal offence, or its reform, in order to satisfy the minimum criminalisation requirement. They do not take into consideration the general principles of criminal law, or their effect on the international obligation. Even where the effort in creating a minimum level of criminalisation is at its greatest, the living system in which the model offence is inserted concretely influences its scope.

This problem typically finds expression at an *ex ante* level: i.e. the lack of harmonisation of the general principles of criminal law. However, it is difficult to predict, at least in the near future, any harmonisation of the general part of the domestic criminal law of States. This is even true of the EU – a geographical area where the States enjoy a close legal and political proximity. Indeed, the general part represents the very foundation of a State's legal tradition and is jealously protected from external modifications. Furthermore, most alterations of a general principle reverberate throughout the whole special part of the criminal code, substantially modifying the entire criminal system.[154]

In order to avoid excessive differences in the concrete scope of the norm, two solutions could be envisaged. The first solution is to provide precise mechanisms to deal with those aspects of international legislation that may lead to incoherency in their domestic implementation; or at least to offer some guidance in non-binding, accompanying reports, such as the report associated with the

---

[151] See, for instance, the subjective element of the offence, or the law of attempt. See G. Fletcher, *Basic Concepts of Comparative Law* (OUP, 1998), "Culpability and the Forms of Mens Rea" (pages 111-129), "Harm and the Law of Attempt" (pages 171-187). See also S. Summers, C. Schwarzenegger, G. Ege and F. Young, *The Emergence of EU Criminal Law* (Hart Publishing, 2014), 261ff.

[152] See N. Boister, "'Transnational criminal law'?" (2003) 14 European Journal of International Law 953, 958; K. Ambos, 'Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections', (2005) 12 Maastricht journal of European and comparative law 173; L. Gröning, 'A Criminal Justice System or a System Deficit? Notes on the System Structure of the EU Criminal Law', (2010) 18 European Journal of Crime, Criminal Law and Criminal Justice; André Klip (ed), *Substantive Criminal Law of the European Union* (Maklu, 2011), 228; J. Blomsma, *Mens rea and defences in European criminal law* (Intersentia 2012); F. Rossi, 'The European harmonisation of the general part of criminal law' (2017) 5 Rivista Italiana di Diritto Pubblico Comunitario 1077.

[153] Analogously, Article 83 TFEU, which represents the legal basis of an EU criminal competence, limits the criminal scope EU Law to the establishment of "minimum rules concerning the definition of criminal offences and sanctions".

[154] Indeed, historically there has been a regular exchange of ideas and mutual influence between criminal law systems (also due to "hard" legal transplants following military conquest), conducive to a certain degree of approximation of the general principles of criminal law.

CoE Convention.[155] The second solution is to consider domestic norms' compliance with international obligations both on the letter of an offence and, *ex post*, on its concrete applicative scope. This solution may require a higher dose of comparative analysis than the mere examination of the norm. It was not endorsed by the 2008 Report on the implementation of the EU Framework Decision on attacks against information systems, which "focuses mainly on the formal level of implementation of the Framework Decision's criminal law provisions" and states that "actual application of those rules is beyond the scope of this report".[156] Conversely, the 2017 Report on the implementation of Directive 2013/40/EU included in the analysis national legislations, "court decisions and – where appropriate – common legal theory"[157], thereby demonstrating higher consideration to the concrete scope of the norm.[158]

II.II.IV. HUMAN RIGHTS AND LIMITS TO CRIMINALISATION, IN PARTICULAR THE PRINCIPLES OF PROPORTIONALITY AND ULTIMA RATIO.

Traditionally, international criminal law instruments aim at providing a "minimum" standard of criminalisation, in order to fulfil a series of mutual interests in the transnational repression of crime. The limits of criminalisation – in particular the fundamental principle that criminal sanctions should be imposed only as a last resort (principle of necessity or *ultima ratio*), in proportion to the gravity of the conduct (principle of proportionality) and, more generally, should not excessively affect the fundamental rights of the individual involved – do not find a precise expression within the international instruments. The space over and above the minimum level of criminalisation is largely left to individual States to determine internally, although such a limit may derive from international human rights obligations.

---

155 CoE, *Explanatory Report to the Convention on Cybercrime* (n 85).

156 See EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM(2008) 4488 final, 4. On this point, see infra Chapter xxx.

157 EU, *Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, COM/2017/0474 final, at 5.

158 Major attention could be possibly expected from the European Court of Justice, that, since December 2014, may review the correct implementation of the EU criminal instrument. With the Treaty of Lisbon, and the abolishment of the three pillars structure, the normal powers of the Commission and of the Court of Justice are applied to the acts in the fields of Justice and Home Affairs, in the same way as in the other areas of EU law. From December 2014 (due to Article 10 of the Protocol on Transitional Provisions, which had frozen such powers for five years), the Commission may thus activate an infringement proceeding if the criminal provisions of the EU law have not been correctly implemented.

If the minimum standard is an ineluctable starting point, States are free to extend their criminal law further, by increasing the scope of criminalisation, or providing for harsher sanctions.[159] However, this margin cannot be seen as a "'*carte blanche*' to create an excessively repressive system"[160]. The main multilateral instruments on cybercrime show a sensibility towards stimulating a *de minimis* approach (e.g. in the EU instruments), providing a set of optional elements that qualify the offence, and offering guidance with regard to additional aspects of specific crimes, including human rights, necessity, and proportionality considerations (e.g. in the Explanatory Report to the CoE Convention).

In any case, the minimum core provided by the international instruments remains broad. It covers a wide range of different behaviours (from terrorists hacking into critical infrastructures, to scholars breaching the terms and conditions of online scientific databases). Suggested penalties are often relatively high. The space for a *de minimis* approach is practically very narrow.

The mutual interests in the transnational prevention and repression of cybercrime.

Cybercrime is a transnational crime *par excellence*.[161] The use of digital technologies makes the crime transcends the geopolitical borders in its preparation (e.g. hackers located in different jurisdictions planning online an attack), in its commission (e.g. *iter criminis* passing through servers located in different jurisdictions), and in its effects (e.g. cyberattacks targeting computer systems located in different jurisdictions). A purely domestic response to the crime is bound to be ineffective. The prevention and repression of cybercrime essentially requires the setting of a transnational minimum level of criminalisation and the development of effective tools of interstate cooperation.

Both the CoE Convention and the EU cybercrime instruments aim to enhance international police and judicial coordination and assistance.[162] These instruments stimulate cooperation directly, via provisions on traditional and cyber-specific tools of police and judicial mutual assistance. They also do it indirectly, inducing a common minimum standard of criminalisation. This common standard may be necessary to overcome the traditional limits of cooperation – in particular the double criminality principle. As an example, the 2005 Framework Decision on attacks against information systems was necessary to integrate the expression "computer-related crime", contained in Article 2.2

---

[159] See F. Calderoni, *Organized Crime Legislation in the European Union* (Springer 2010), 5.

[160] See A. Klip, *European Criminal Law: an Integrative Approach* (Intersentia 2009), 162.

[161] See EU, *Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, 28.3.2012 COM(2012) 140 final: "No crime is as borderless as cybercrime".

[162] Also due to the typical volatility of data and electronic evidence.

of the Council Framework Decision on the European Arrest Warrant. The setting of common cyber norms was thus of pivotal importance in making the European Arrest Warrant system fully operative with regards to such offences.[163]

Furthermore, the international cybercrime treaties have a transnational prevention aim.[164] With the setting of a common minimum standard of criminalisation, these instruments create a "prohibition regime"[165]. They envisage a wide repression of cybercrimes and eliminate or minimise potential havens for cybercriminals. States have a specific interest in creating an area of common criminalisation of cybercrime in order to avoid attacks being launched from the territory of other neglectful States.[166]

The minimum criminalisation standard is related to these mutual interests. In setting this standard, it is required that the drafting States understand the desired threshold on which they want their mutual cooperation to work efficiently, and other States to repress cyber conducts which *in abstracto* may have repercussions on their territory.

---

[163] See P. De Hert, G. González Fuster and B. Koops, 'Fighting cybercrime in the two Europes. The added value of the EU Framework Decision and the Council of Europe Convention' (2006) 77 Revue Internationale de Droit Pénal 503, 506-7.

[164] The CoE Recommendation was enacted as an "appeal to those responsible for the development of national criminal policy and its conversion into legal provisions to allow themselves to be guided by this European consensus", in order to "prevent abuses from being shifted to and committed in those states whose criminal law previously exhibited loopholes" and "facilitate[s] international co-operation" (CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 33). Likewise, the aim of the CoE Convention was "to prevent and suppress computer or computer-related crime by establishing a minimum standard of relevant offences", in order to "alleviate[s] the fight against such crimes on the national and international level" and "prevent abuses from being shifted to a Party with previous lower standard" (CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), at §33). According to the 2002 Proposal for a Council Framework Decision on attacks against information systems "Member States' laws in this area contain some significant gaps and differences (…). Perpetrators of these offences need to be identified, brought to justice, and the courts need to have appropriate and proportionate penalties at their disposal. (…) In addition, these gaps and differences could act as a barrier to effective police and judicial co-operation in the area of attacks against information systems. Attacks against information systems could often be trans-national in nature, and would require international police and judicial co-operation. Approximation of laws will therefore improve this co-operation by ensuring that the dual criminality requirement is fulfilled" (EC, *Proposal for a Council Framework Decision on attacks against information systems* (n 112), §1.5).

[165] See E. A. Nadelmann, 'Global Prohibition Regimes: The Evolution of Norms in International Society', (1990) 44 International Organisation 44, 479. See also F. Gregory, 'Private Criminality as a Matter of International Concern', in J. W. E. Sheptycki (ed.), *Issues in Transnational Policing* (Routledge 2000); N. Boister, "'Transnational criminal law'?" (n 144), 955

[166] Traditionally, such interest is reciprocal within a specific regional area, since "physical" transnational crimes tend to affect neighbouring geographical zones. In cyberspace, conversely, the concept of "neighbourhood" assumes a completely different meaning. Passing through the web, cyberattacks are not affected by distances or political borders. Consequently, the "prohibition regime" should be extended as much as possible. As pointed out *infra*, an effective legal answer to cybercrime possibly require for an international extension of the harmonisation effort. With regards to this point, the CoE Convention, having a quasi-international reach, could appear more effective than the EU instruments.

Human rights as limits to criminalisation.

The international cybercrime instruments set the minimum criminalisation standard as a "departing point". From there, State members can go further, broadening the scope of criminalisation, or providing for harsher sanctions.[167] The natural borders to such action are defined by the human rights of the individuals involved, in particular those enshrined in the general principles of criminal law, such as the principles of *ultima ratio* and proportionality.

Human rights standards are traditionally incorporated into international criminal treaties only as an "indirect" limit to criminalisation, which works exclusively at the national level. As pointed out by Boister, "the problem is that the conventions are adopted at the international level, and then applied at the national level, but human rights only come into play, if at all, at the national level, reactively rather than proactively." [168]

The CoE Cybercrime Convention does not provide for an express protection of human rights involved in the criminalisation of cybercrime. It merely includes a traditional, "indirect" incorporation of external human rights obligations, which does not entail any direct limit to the scope of the provisions.[169] Article 39 (3) of the Convention states in vague terms that "nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party". Furthermore, the Preamble of the Convention stresses the "need to ensure a proper balance between the interest of law enforcement and respect for fundamental human rights" – in particular the European Convention on Human Rights, the International Covenant on Civil and Political Rights, and other applicable international human rights treaties. The incorporation of external human rights obligations appears formulated as a *caveat* to the States, to be considered at the domestic level. Eventually, possible conflicts between human rights and international obligations

---

[167] See F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 5.

[168] N. Boister, "'Transnational criminal law'?" (n 144), 959: "Moreover, the conventions encourage a "law and order" attitude from state parties which may cause them to go further than strictly obliged to, with negative consequences for individual rights".

[169] A stronger relation criterion is envisaged for the procedural provisions of the treaty. CoE, *Convention on Cybercrime* (n 81), Article 15 – Conditions and safeguards: 1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

stemming from the CoE Convention can be brought before the international adjudication bodies established by international human rights conventions. It is important to consider, however, that several States parties to the Budapest Convention are not members of the Council of Europe nor parties to its European Convention on Human Rights.

Like the CoE Convention, the EU instruments on cyberattacks do not contain any express protection of human rights involved in the criminalisation of cybercrime. The primary place for assessing possible conflicts between human rights and EU obligations remains the domestic system. From there, such conflicts can be brought before the Court of Justice of the European Union, or the European Court of Human Rights. Incidentally, one should note that after the Treaty of Lisbon, and the abolishment of the three-pillar structure, the normal powers of the Commission and of the Court of Justice are also applied to acts in the fields of Justice and Home Affairs, similarly to the other areas of EU law. From December 2014[170], the Commission may activate proceedings against an infringement if the criminal provisions of EU law have not been correctly implemented.

However, within the EU normative system direct influence on the substantive provisions of the EU instruments is also provided for by the supremacy criterion between primary and secondary law. The EU cyber instruments are in fact part of the same normative system of the human rights enshrined in the Charter of Fundamental Rights of the European Union (and in the general principles of EU Law), and hierarchically subject to them.[171] These rights are considered the ineluctable heart of the EU legal structure. Respecting these rights is a necessary precondition for the legality of any EU act and its national implementation, which is monitored by the Court of Justice.[172]

Several fundamental rights enshrined in the EU system are relevant to criminal law. Of general importance with regard to overcriminalisation are the principles of proportionality and *ultima ratio*. The principle of proportionality between penalties and criminal offences is recognised by Article 49(3) of the Charter of Fundamental Rights and "enshrined in the common constitutional

---

[170] Due to Article 10 of the Protocol on Transitional Provisions, which had frozen such powers for five years. EU, *Consolidated version of the Treaty on European Union - Protocol (No 36) on transitional provisions*, OJ C 115 2008.

[171] The Charter has become legally binding on the EU States Members with the Lisbon Treaty.

[172] See inter alia P. de Hert, 'EU criminal law and fundamental rights', in V. Mitsilegas, M. Bergström, & T. Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edwar Elgar, 2016), 109ff; D. Ritleng, 'The Contribution of the Court of Justice to the Structuring of the European Space of Fundamental Rights', (2014) 5 New Journal of European Criminal Law 507. See also Article 51 of the Charter, which prescribes that the fundamental rights enshrined within it apply only to persons affected by a measure of an EU institution or Member States' action or omission deriving from an obligation under EU law.

traditions of the Member States and in the case-law of the Court of Justice of the Communities"[173]. A specific attention towards a balanced modulation of the punishment, which must be dissuasive and effective, but also proportional, is expressed with regards to the national enforcement of EU law by the so-called Greek Maize criterion.[174] It is also mirrored in the 2005 Framework Decision and 2013 Directive on cyberattacks, which require member States to adopt "effective, proportional and dissuasive penalties".[175]

Although not explicitly envisaged by the Charter of Fundamental Rights, the *ultima ratio* principle permeates the entire EU human rights system. [176] This principle acknowledges the depressive effect of criminal justice on a series of human rights.[177] First, it demands the use of criminal law as a last resort, only to be used when no less restrictive means can achieve the same result. Second, it requires that criminal law is employed only to enforce the most serious harms or endangerments to a legal interest. As such, it works in parallel with the principle of proportionality in setting a limit to criminalisation, preventing its overextension. Third, in the EU system, the *ultima ratio* principle is intimately connected to the principles of conferral, subsidiarity and proportionality (Article 5 Treaty on European Union), which set the boundaries of the competences of the European Union. The *ultima ratio* principle thus requires the European legislator to act only when it is best placed to afford criminal law protection to a legal interest.

The EU instruments also have a strong connection with the European Convention on Human Rights (ECHR), even more than the CoE Cybercrime Convention. Article 6(3) of the Treaty on European Union refers to the ECHR as part of the general principles of EU law. Article 53 of the European Charter contains a non-regression clause, by which the Charter's provisions must not be interpreted as "restricting or adversely affecting" the human rights recognised in the ECHR. Such an implicit relation is recalled in the preamble of the EU Directive on cyberattacks, which states

---

[173] EU, *Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007,* Explanation to Article 49. See also EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*, COM(2011)573, 20 September 2011, 7.

[174] CJEU, *Commission v Greece (Greek Maize)*, Case C-68/88, [1989] ECR 2965. See also A. Klip, *European Criminal Law: an Integrative Approach* (n 160), 74, 75.

[175] EU, *2005 Framework Decision on attacks against information systems* (n. 82), Art. 6; EU, *2013 Directive on attacks against information systems* (n 83), Article 9. As pointed out by Advocate General Kokott, "a penalty is proportionate where it is appropriate for attaining the legitimate objectives pursued by it, and also necessary" (CJEU, *Criminal proceedings against Silvio Berlusconi (C-387/02), Sergio Adelchi (C-391/02) and Marcello Dell'Utri and Others (C-403/02)*, Opinion of Advocate General Kokott of 14 October 2004).

[176] See inter alia ECJ, Commission v. Council, C-440/05, ("ship-source pollution case") § 71; S. Melander, 'Ultima Ratio in European Criminal Law' (2013) 3 Oñati Socio-Legal Series 1.

[177] Chiefly the right to liberty and security, which "must be respected particularly when the European Parliament and the Council adopt legislative acts in the area of judicial cooperation in criminal matters" (EU, *Explanations relating to the Charter of Fundamental Rights* (n 173), Explanation on Article 6 — Right to liberty and security).

that "this Directive seeks to ensure full respect for [human rights and fundamental freedoms and (…) the principles recognised in particular by the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms][178] and must be implemented accordingly".

With regards to the principles of proportionality and *ultima ratio*, the ECHR system does not expressly recognise them as direct or corollary "rights" in themselves, but rather as immanent limits to the compression of human rights. The severity of a criminal instrument is thus assessed *vis-à-vis* the proportionality of its interference with existing Convention rights.

The direct relationship between EU law and human rights obligations (deriving both from the EU and the ECHR system) requires a balance between criminalisation and human rights at the drafting, implementation, and applicative levels. Such balance is both expressed within and by the domestic system in the implementation of the instruments, and directly within and by EU law, "proactively rather than reactively"[179]. It thus demands that major attention be paid to aspects that are recognised to lead to risks of overcriminalisation at the legislative and judicial levels.

II.II.V. A COMMON SUPRANATIONAL INTEREST IN THE PROTECTION OF NETWORKS AND INFRASTRUCTURES?

Traditionally, international influences on national criminal law are regarded with distrust. Yet, it is undeniable that these influences are growing. This is not only due to the normative evolution of regional and international legal systems, and the extended competence of their judicial apparatus. It also appears to be a natural reflection of the emergence of common supranational interests.

With regard to such interests, the aim of harmonisation is extending beyond traditional mutual cooperation to create a shared protection of regional or international legal interests, and eventually direct supranational adjudication and prosecution of crimes harming or endangering such interests.

In the EU, the seed of this extension can be found in the words of Article 83(1) Treaty on the Functioning of the European Union, which recognises the "need to combat particularly serious

---

[178] EU, *2013 Directive on attacks against information systems* (n 83), Preamble § 29: "This Directive respects human rights and fundamental freedoms and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, including the protection of personal data, the right to privacy, freedom of expression and information, the right to a fair trial, the presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties."

[179] See N. Boister, "'Transnational criminal law'?" (n 144).

crime with a cross-border dimension *resulting from the nature or impact of such offences or from a special need to combat them on a common basis*".[180] The list of these serious crimes (the so-called "eurocrimes") includes "computer crime".

A step beyond traditional harmonisation has been taken in the area of EU financial interests, which are recognised as legal goods over which the EU system has exclusive competence. An increase in the protection of these interests took place in 2017, with a Directive on the fight against fraud to the Union's financial interests by means of criminal law.[181] Importantly, both a directive and a regulation were initially identified as the appropriate legislative instruments to achieve this protective aim. Although the former was preferred, the latter was considered compliant with the EU proportionality principle, which states that the content and form of EU action shall not exceed what is necessary to achieve the objectives of the Treaties. The interests at stake were thus recognised as being of sufficient relevance to directly impose criminal provisions and sanctions to member States.[182]

Clearly, where regional or international legal interests are identified, it is possible to notice a tendency towards an integrated system of protection for common legal interests. At the normative level, this tendency is coupled with a modification in the relationship between the peripheral (State) and central (EU) jurisdictions. The latter is acquiring a major interest in regulating, with additional precision, the scope of key criminal norms.[183] Currently, on the basis of the principle of loyal cooperation, enforcement is delegated to Member States, which are required to take all measures necessary to guarantee the application and effectiveness of EU law, and ensure that "infringements of (EU) law are penalised under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance and which, in any event, make the penalty effective, proportionate and dissuasive".[184] Eventually, at the enforcement level, the central jurisdiction may wish to take upon itself the responsibility for the direct prosecution of crimes affecting its "common" interests. With regard to EU financial interests,

---

[180] Emphasis added. See S. Ruggeri (eds), *Human Rights in European Criminal Law: New Developments in European Legislation and Case Law after the Lisbon Treaty* (Springer, 2015), 206 ff.

[181] EU, *Directive 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law*, OJ L 198, 28.7.2017.

[182] EU, *Report on the proposal for a directive of the European Parliament and of the Council on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA,* COM(2013)0042 – C7-0033/2013 – 2013/0023(COD), A7-0018/2014, 10.1.201, § 4.

[183] See P. Caeiro, 'The relationship between European and international criminal law (and the absent(?) third)', V. Mitsilegas, M. Bergström, & T. Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edwar Elgar, 2016), 582 ff.

[184] ECJ, *Commission v. Greece*, Case C-68/88, [1989] ECR 2965, § 23.

this is signified by the creation of the European Public Prosecutor's Office, which will offer an independent prosecution at the European level of conducts harming such interests.

Although not yet fully recognised at the normative level, the increasing regional and international value of certain "digital" interests is undeniable. Today, information systems and networks are strictly interconnected and interdependent.[185] Computer systems are increasingly carrying out functions that have significant influence beyond the territory of the State within which they are physically located. In particular, certain infrastructures essential for the maintenance of vital social functions, such as energy, communication or transport, are becoming of regional or global value, and increasingly dependent on information technology.[186] They are therefore vulnerable to cyberattacks. The disruption or destruction of such infrastructures has significant cross-border impacts. Consider the 2006 European Blackout, when a shutdown of a high-voltage line in Germany resulted in massive power failures in France Italy, Spain, Portugal, the Netherlands, Belgium, Austria, and Morocco.[187] Similar was the 2013 Spamhaus DoS attack, when a non-profit anti-spam group (Spamhaus) was a victim of one of the largest computer attacks on the Internet, causing extensive web traffic congestion worldwide, and almost disrupting critical Internet Service Providers (ISPs) [188].[189]

Some types of cyber acts – and in particular large-scale attacks against digital infrastructures – tend to "touch" and produce effects in more than one State. Furthermore, they can directly harm or endanger values of a regional or global character. As a consequence, regional or global common interests in the effective prevention and repression of these acts are emerging.

References to such common interests can be found in the EU instrument on cybercrime. The preamble to the 2013 Directive states that: "Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of information systems should form part of an effective

---

[185] In this sense, already the EU, *Proposal for a Council Framework Decision on attacks against information systems* (n 112), §1.

[186] See EU, *Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector*, 3.4.2019 C(2019) 2400 final.

[187] See E. Van der Vleuten and V. Lagendijk, 'Transnational infrastructure vulnerability: The historical shaping of the 2006 European "Blackout"' (2010) 38 Energy Policy 4, 2042-2052.

[188] An Internet service provider is an entity that provides services for accessing or using the Internet. Internet service providers may be classified according to the service they offer. The most important types of ISPs are: access providers, which provide Internet access; mailbox providers, which provide services to send, receive, and store emails; hosting providers, which provide online storage services.

[189] See, inter alia, M. Prince, 'The DDoS That Almost Broke the Internet' (Cloudflare 27 March 2013) <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/>.

comprehensive framework of prevention measures accompanying criminal law responses to cybercrime."[190]

Since 2004, with the Communication of the Commission on Critical Infrastructure Protection in the Fight against Terrorism[191], the EU has paid particular attention to cyberattacks against critical infrastructures. The strategy to protect critical infrastructures found its cornerstone in the Council Directive 2008/114/EC, which sets up a procedure for identifying and designating European critical infrastructures and provides an approach for assessing the need to improve their protection.[192] The EU criminal law on attacks against information systems has to be read as a part of the EU policy of providing protection to the common European critical infrastructures, networks, and information systems. A combined analysis of these factors could highlight elements of the EU instruments on cyberattacks that incorporate aspects of a common supranational criminal policy. Arguably, such integration will become increasingly relevant in light of continual digital evolution.

So far, the increased sensibility towards such common interests has merely translated in an augmented protection of computer systems and data, as well as harsher penalties, driven by the EU instruments. One should notice, however, that the more regional and international interests are digitalised, the more international influence on their criminal protection is to be expected. This influence may lead to a stronger harmonisation of cybercrime law, narrower international obligations, and eventually a direct supranational prosecution of cybercrime.

---

190 EU, *2013 Directive on attacks against information systems* (n 83), Preamble § 2.

191 EU, *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, COM/2004/0702 final.

192 EU, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, OJ L 345, 23.12.2008, 75–82. See also EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",* SEC(2009) 399, SEC(2009) 400, COM/2009/0149 final.

II.III. CRIMES AGAINST THE SECURITY OF COMPUTER SYSTEMS AND DATA: ILLEGAL ACCESS TO A COMPUTER SYSTEM.

The terms "cyberattack" and "computer hacking" are typically used to define the same genus of crimes. The term "cyberattack" hints at the modalities of the crime: an "attack", a violent and damaging act, committed with the use of and against "cyber" goods, i.e. computer system and data. Referring to the same behaviours, the term "computer hacking" is more focused on criminological aspects. It defines the typical (almost mythological) perpetrator of the crime: the hacker. However, "hacker" is a rather vague, media-favoured term, and indicates a plethora of diverse cyber actors.[193] Cyberattacks can be considered as cyber offences *stricto sensu*: they are new, cyber specific, technology-related forms of criminal activity that affect new legal interests. These offences basically involve every "abuse" of computer systems and data, through illegal access to, alteration of, and damage to those systems. More precisely, they encompass: exploiting computer vulnerabilities[194], illegally accessing a computer system or data, damaging them, and hindering their proper functioning.

---

[193] Due to the semantic misperception related to the word "hacker", this term has acquired an extremely vague meaning. It includes people with different technological skills, criminal intentions and motivations. Numerous studies have attempted to define and categorise further the hacker subcategories in order to better understand the "computer underground" panorama. Various categorisations exist. Most classifications take into consideration the technical skill and the experience of the hackers. A hacker can vary from a highly skilled person (a computer "wizard") to a simple neophyte armed with basic technical skills. The lower tile of the hacking community is usually called a "novice". Novices often rely on the existence of available tool kits, programs and scripts to conduct their actions. Thus, in the hacker jargon, they are also called "script kiddies". When moved by a desire to learn, they may observe, study and follow the "elite hackers". Each hacker may learn specific computer skills, depending on the type of activity he/she usually conducts. Thus, a necessary element of distinction is the "sector" in which the different type of hacker operates. For instance, in one of the first taxonomical studies of the phenomenon, Hollinger (R. C. Hollinger, 'Computer hackers follow a Guttman-like progression' (1988) Sociology and Social Research, 199) divided hackers in the following way: "pirates", who illegally copy and distribute material protected by copyright; "browsers", who gain unauthorised access to the computer system to browse through private files; and "crackers", who aim to damage or alter computer data and systems. Other examples are the "virus writer", specialised in writing (and diffusing) malware, and "penetration testers" or "bug hunters", who access computer systems to search for vulnerabilities. See *inter alia* M. K. Rogers, 'A two-dimensional circumplex approach to the development of a hacker taxonomy' (2006) 3(2) Digital Investigation 97, 98; S. LN Hald and J. M. Pedersen, 'An updated taxonomy for characterising hackers according to their threat properties', in *14th International Conference on Advanced Communication Technology* (IEEE 2012), 81, 83 Table 2; B. Landreth, *Out of the Inner Circle: a Hacker's Guide to Computer Security* (Microsoft Press 1985); C. Meyers, S. Powers and D. Faissol, 'Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches' (U.S. Department of Energy
Office of Scientific and Technical Information 2009).

[194] See *supra* n 9.

The CoE Convention on Cybercrime provides for a precise categorisation of the above-mentioned criminal conducts through an object-focused approach. This categorisation, subsequently adopted at the European Union level, revolves around the target of the crime and the legal interest(s) affected.[195]

This genus of crimes can thus be categorised as conduct that directly targets computer systems and data, and the legal interest of their "security" in its main aspects of confidentiality, integrity, and availability.

Within this category of crimes, a further classification takes into account the different behaviours that could harm or endanger such interests. Cyberattacks are thus decomposed into single substantive offences. Their conceptualisation revolves around four main criminal conducts: illegal access to computer systems, interception of data, interference with data, and interference with computer systems. To this set of offences is to be added the complementary offence of misuse of devices, which advance the moment of criminal repression to preparatory acts (i.e. the unauthorised possession, production, sale, procurement for use, import, distribution, or otherwise making available of a device aimed at providing access to a computer).

This categorisation is envisaged by the CoE Convention and the EU instruments but is not necessarily followed at the domestic level. [196] However, it permits a clear identification of the various elements of cyberattacks. It will be therefore adopted for the scope of this work.

---

[195] Besides providing for rationalisation, its importance relates to the fact that, traditionally, cyber offences hardly contain, in the structure of the norm, an explicit or implicit reference to the legal interests protected. See I. Salvadori, 'L'accesso abusivo ad un sistema informatico o telematico" (n. 138), 127-128.

[196] At the domestic level, this categorisation was fully embraced by the Belgian legislator, which, in 2000 (thus before the enactment of the Budapest Convention) created a new Title IXbis in its criminal code, containing the basic cyber-specific offences. Belgium, *Code Pénal*, Titre IXbis. - Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

II.III.I. ILLEGAL ACCESS AS A PARADIGMATIC EXAMPLE OF A MINIMUM CRIMINALISATION OFFENCE WITH A "VARIABLE GEOMETRY".

Among the different criminal conducts that may harm or endanger the security of computer systems and data, illegal access to a computer system enjoys a prominent position. This conduct is the primary and fundamental block of a systematic legal construction of computer hacking. Even criminologically, access is the fundamental action of most cyber criminal behaviours. Cybercrimes ordinarily begin with an illegal access to computer systems or data. As an example, a computer "sabotage" has a logical antecedent in the illegal access to a computer: a malware may be installed onto a computer system (illegal access) and damage data contained therein (data interference).

The offence is constructed around a core act of access, and its scope is influenced by a series of subjective and objective elements which qualify the offence. Such elements are not precisely delineated by the international cyber instruments and find diverse application in domestic systems.[197]

However, these elements hold a pivotal role in the overall cybercrime framework. Access to computer system and data is a common action in cyberspace, which does not *per se* express criminal intentions.[198] The exact borders of its criminalisation are of fundamental importance in defining legal or illegal activities in cyberspace. By narrowing or expanding the scope of the offence, these elements define illegal behaviour in cyberspace. Furthermore, they blur the distinction between illegal access and the possible illegal conduct that could be engaged in subsequently, once inside the system.[199]

The 1989 CoE Recommendation on Computer-related Crime made the first moves towards the criminalisation of illegal access. At that time, likely due to the crime's scarce empirical relevance, the

---

[197] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices,* CoE Project on Cybercrime, Discussion Paper (2008), 16-17.

[198] For instance, accessing a computer system in order to explore it (and find its flaws, with benevolent intentions) is the typical action of the hacker subculture. See E. Goldstein, 'The Constitution of a Hacker' (1984) 2600 The Hacker Quarterly: "The realistic way for the owners of large computer systems to look at this is to regard hackers as necessary security checks. That's right. Necessary because if the hackers weren't the ones to break in, who would be? Let's assume that hackers had never even tried to break into the Memorial Sloan-Kettering Cancer Center computer. Someone else would have, because the system was practically wide open. And maybe they would have had a reason to get into the system to do various nasty things. But now, because of what the hackers did, the Sloan-Kettering system is more secure. One could almost say that a person with hacking abilities has an obligation to try and get into as many different systems as he can."

[199] See UNODC, *Comprehensive Study on Cybercrime* (n 66), 83.

criminalisation of such behaviour was rare. Only few domestic systems worldwide (Denmark, France, Sweden, and the US) provided for an autonomous criminalisation of illegal access. The drafting Committee envisaged abusive access in its minimum list of offences, suggesting that States introduce it into their penal codes. According to the accompanying Report: "The committee is convinced that the dangers arising from acts of hacking may increase in the future and therefore proposes that all member States should undertake to prevent and combat such dangers, not only by improving security measures but also by criminalising at least qualified acts of so-called 'computer trespass'"[200].

In the Recommendation, illegal access was not given the central relevance that it would later acquire in the CoE Convention and the EU instruments, possibly due to subsequent technological and criminological evolution. The Committee did however show sufficient awareness of the main controversial issues related to the offence of illegal access. Nonetheless, it did not take a stable position on the constituent elements of the norm, providing scant guidance to States on the surrounding aspects of the issue – in particular, on the substantive element of the crime.

Vagueness in the wording around the qualifying elements of the offence, and the use of polysemic words or technical terms to be specified at a domestic stage, is repeated in the subsequent binding instruments on cybercrime.

The legal interest protected.

The offence of unauthorised access to computer systems perfectly exemplifies the crucial role paid by the protected legal interest within the structure of cyber offences.

At the international level, the first specification of the legal interest protected by the offence is to be found in the 1989 CoE Recommendation.[201] The recommendation presents a fundamental dichotomy of interests and assimilates two disparate concepts. According to the instrument, the offence of unauthorised access to computer system is aimed at protecting "the security of the

---

[200] CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 51.

[201] Although the instrument did not offer the same categorisation according the legal interests protected to be found in the subsequent international cyber instruments.

computer system and the inviolability of the computer domicile".[202] However, a variation in the emphasis given to one or the other interest substantially influences the offence's construction and scope.

If the offence is aimed at protecting the security of the computer systems (or even, from a more recent perspective, of networks), it represses acts of concrete endangerment to the confidentiality, integrity, and availability of computer systems. The conduct should express a possible future harm to such interests. Accordingly, the objective and subjective elements of the offence should be modulated so as to cover conducts that present that level of endangerment.

On the other hand, an offence aimed at protecting the computer domicile is constructed as a digital transposition of physical trespass on private property. Such offence focuses on the protection of the property rights of the computer system's owner, and its *ius excludendi alios*.[203] The offence's scope is therefore less prone to qualitative narrowing. Any breach of a computer domicile tends to be repressed by the norm, irrespective of the actor's aims, or of the act's endangerment to the confidentiality, integrity, or availability of the computer system and data. The protection of these latter interests will be requested to the subsequent set of cyber offences. The relation between the offences composing the cybercrime framework (in particular, illegal access and interference) will be thus modified. The overlapping area between them may be contracted, producing a relation of subsequentiality, rather than supplementarity.

An interesting compromise in this area is provided by the German system, which criminalises illegal access in a strongly qualified modulation. *Strafgesetzbuch* § 202a(1) punishes unauthorised access and obtainment of data that are not intended for the actor. The offence protects an area of privacy of the computer system's owner, considered to be his/her exclusive ownership and control over data

---

[202] CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 51. The EU cybercrime instruments do not precisely indicate the legal interests protected by their provisions. *Per contra*, the Explanatory Report of the CoE Convention does provide for such clarification. Interestingly, the Report recognises that the "interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner" is the protected interest of the unauthorised access offence (CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 44). Such formulation suggests framing the offence as a crime of result, covering every intrusion to computer systems that creates "disturbance". Therefore, it requires a harm to the availability of computer systems. The normative framework of the CoE Convention, however, highlights the early scope of the offence: the exclusion of its criminalisation as an attempt, provided for Article 11.2 of the Convention, seems to confirm that illegal access to computer system should be considered in its early protection (mere endangerment) of the general security of computer systems.

[203] For instance, the Italian offence of "*accesso abusivo ad un sistema informatico o telematico*", provided by Article 615ter of the Italian Penal Code, aims to protect the "computer domicile" pertaining to a physical or juridical person, which is considered as the *dominus* of this digital locus. See *ex plurimis* ITA, Corte di cassazione, *Judgments n. 3065 and 3067*, 4 October 1999 (although different interpretations of the legal interest protected by the norm can be found in the case law of the Supreme Court). See also R. Flor, 'Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios' (2005) 1 Diritto Penale e Processo 85.

(*Herrschaftverhaltnis*).[204] However, such a dimension is essentially associated with privacy aspects. The central core of the legal interest protected by the *Strafgesetzbuch* is therefore related to computer systems and data in their identity as containers of personal information.[205] The offence is entitled "data espionage" (*Ausspähen von Daten*) and is inserted in the title on "*Verletzung des persönlichen Lebens - und Geheimbereic*h" (Violation of personal life and secrets). It therefore loses its anticipatory function in favour of a protection of the confidentiality of data. It is narrower than the offences constructed around the nebulous concept of the "computer domicile", and substantially restricts access to data intended to remain confidential.

The Spanish system follows an even more radical approach. Article 197 of its *Código Penal* criminalises the act of gaining illegal access to computer systems. The offence is directly outlined in the part of the code that deals with crimes against privacy.[206] Similar to the German system, it only covers "reserved" data which the offender accesses without the consent of the victim. However, its scope is limited to access to information regarding the private life of the victim.[207]

The material element.

Accessing and maintaining without right…

The core constituent of the offence's *actus reus* of unauthorised access is the access to a computer system. Unlike most US State legislations,[208] no European cyber legislation defines the meaning of the word "access". In any case, the term has to be interpreted as the establishment of functional communication with the computer's software. Physical access to hardware (which is covered by traditional criminal norms) has to be excluded.[209]

An important issue relates to the *unauthorised* or *without right* nature of the access. This issue is recurrent in cybercrime law. However, with regard to this specific norm, it is of critical importance,

---

[204] See Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal*, Rapports nationaux, Colloque Préparatoire Section I. Vérone (Italie), 28-30 November 2012, Droit Pénal Général, Marco Gercke, Germany, 4. See also E. Hilgendorf, '§ 202a Ausspähen von Daten', in *Leipziger Kommentar* (De Gruyter 2010), 1440-1.

[205] See A. Marberth-Kubicki, *Computer-und Internetstrafrecht* (CH Beck 2010), 42ff.

[206] Spain, *Código Penal*, Título X - Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Capítulo Primero - Del descubrimiento y revelación de secretos.

[207] See J. De Otaola Zamora and P. Letai Weissenberg, *Cyber Law in Spain* (Kluwer Law International 2011), 237.

[208] See O. S. Kerr, 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes' (2003) 78 New York University Law Review 1596; L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 13-14.

[209] See I. Salvadori, 'L'accesso abusivo ad un sistema informatico o telematico" (n. 138), 135.

since the offence is often committed by "insiders" (employees who are authorised to gain access to the system but exceed the terms of their contractual entitlement in order to engage in malicious actions).[210]

The 1989 CoE Recommendation evaluated the nuances of the terms, and deliberately used the syntagma "without right", which is considered to encompass a larger notion than "unauthorised". The formulation proposed by the 1989 CoE Recommendation was endorsed by the CoE Convention and the EU instruments on attacks against information systems. The Explanatory Report to the CoE Convention further considered that this expression is intended to exclude lawful actions undertaken under legislative, executive, administrative, judicial, contractual, or consensual authority, and "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices"[211]. However, the term does not properly encompass all "undesired" behaviours, and it is not expressly including the violation of contractual relations.[212]

On a deeper analysis, the issue of a breach of an authorisation granted under a contractual relation raises further questions. Firstly, should this formulation include both illegal accessing (action) and remaining on the system without consent (omission)? Internationally, illegally remaining in a computer system is separately considered in three multilateral instruments.[213] In the CoE Convention, illegally remaining was explicitly provided in the first drafts, but removed from the final version.[214] Interestingly, national systems may address the problem from a different perspective. For instance, a construction of the offence through an analogy with the crime of physical trespass on private property permits a more stable position on the point. Criminal trespass usually covers both gaining illegal access and remaining on a property without consent of the *dominus loci*, since the *ius excludendi* is the pivotal element of the crime. In Article 615ter of the Italian Penal Code, introduced by Law 547/1993 under the stimulation of the 1989 CoE Recommendation, the offence of abusive access to a computer system is formulated so as to cover both access and remaining without

---

[210] See, inter alia, S. L. Pfleeger, J. B. Predd, J. Hunker, C. Bulford, 'Insiders behaving badly: Addressing bad actors and their actions', (2010) 5 IEEE Transactions on Information Forensics and Security 169.

[211] *Ibid.*

[212] See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 35.

[213] Economic Community of West African States, *Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS* (2011), Article 5; International Telecommunication Union / Caribbean Community /Caribbean Telecommunications Union, *Model Legislative Texts on Cybercrime* (2010), Article 5; African Union, *Convention on Cyber Security and Personal Data Protection,* Art. 29 (1) (c).

[214] See ITU, *Understanding Cybercrime: Phenomena, Challanges and Legal Response* (n 66), 181-182.

consent.[215] Similar formulations are to be found in the French (Art. 323-1) and Belgian (Art. 550bis) systems.

Secondly, it is not entirely clear from the international formulations if and how a misuse of a system by an authorised individual is covered by the offence. In particular, the use of a system for finalities not contemplated by the terms of a contract may find itself on the edges of the illicit area. Consider as an example the act of accessing an online scientific database and using the related material for activities not envisaged by the terms of contract.

Theses issue, of pivotal importance, are thus left for the States to determine.[216] In the Federal U.S. system, the same core concept is expressed by criminalising the act of accessing a computer without authorisation or exceeding authorised access[217].

…in whole or a part of a computer system…

All of the multilateral instruments on the subject provide for the criminalisation of the access to the whole or a part (such as hardware components, traffic data, or content-related data) of a computer system.[218] This specification may cover situations where accessing the computer system is generally authorised, but parts of it, such as specific data, are excluded from the authorisation.[219]

The distinction between the whole and a part of a computer system is not observed by the majority of national systems.[220] For instance, the Italian code envisages a general formulation of access to computer systems and addresses an illegal access to part of them as an excess of authorisation.[221]

The national approaches to this issue are numerous, and may alter the scope of the offence, including or excluding situations in which there is no actual alteration of or access to data. As previously covered here, the German system exclusively focuses on access to data. Similarly, the UK

---

[215] ITA, *Codice Penale*, Article 615ter: "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo…*".

[216] See, on the Italian system, N. Bussolati, 'Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo dell'abusività' (2018) 4 Studium Iuris 428.

[217] See US, *Title 18 US Code*, §1030(a)(2).

[218] See, e.g., CoE, *Convention on Cybercrime* (n 81), Article 2. The Explanatory Report to the CoE Convention specifies that the method of communication with the target (e.g. wireless communication) is irrelevant. See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §46.

[219] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 13.

[220] *Ibidem*; UNODC, *Comprehensive Study on Cybercrime* (n 66), 83; EU, *Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU* (n 149), § 2.2.a. FR, *Code pénal*, Art. 323-1, explicitly envisages such a distinction.

[221] ITA, *Codice Penale*, Art. 615ter.

system covers "computer material"[222], the Armenian Criminal Code "information stored in a computer system"[223], and the Croatian legislation "computer data and programs". These different formulations, often related to the legal interest protected, provide completely different scopes to the offence. For instance, the German and Spanish systems adopt a narrower approach that focuses on the protection of privacy, thus exclusively on data. *Per contra*, legal system providing general protection to computer systems (such as the Italian system, which focus on the *ius excludendi alios* of their owner) criminalises the mere access to computer systems without necessary data retrieval.[224] Liability is therefore activated at an earlier stage of the conduct.

Neither the CoE Convention nor the EU instruments provide for a narrowing of the offence to merely accessing data. However, the former envisages an optional qualitative restriction of the offence to illegal access to networked computer systems. The option permits Parties to exclude from the scope of the norm access to stand-alone systems. However, this option may leave uncovered most illegal access by "insiders". Due to the related economic implications of insider threats,[225] States are unlikely to embrace this nuanced formulation. This option was not implemented in the legal systems of the Parties,[226] and was rejected by the subsequent EU instruments on attacks against information systems.

…protected by security measures (and by infringing such measures)…

A further issue relates to the security measures protecting the computer system. The 1989 CoE Recommendation envisaged a qualitative condition of the presence of security measures protecting the system, and their infringement by the perpetrator. It noted that such condition may work as a stimulus to provide security to computer systems.[227] Conversely, its absence could favour "managerial negligence in the setting up of suitable protection systems".[228]

---

[222] UK, *1990 Computer Misuse Act*, Unauthorised access to computer material.

[223] Armenia, *Criminal Code*, Article 252.

[224] See I. Salvadori, 'L'accesso abusivo ad un sistema informatico o telematico" (n. 138), 139.

[225] See *supra* n 210. See also e.g. S. Morgan, 'Cyber Attacks By Insiders Result In Devastating Costs To Organizations Globally' (Cybercrime Magazine, 11 June 2018) <https://cybersecurityventures.com/cyber-attacks-by-insiders-result-in-devastating-costs-to-organizations-globally/>

[226] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 14.

[227] See, e.g., Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Droit Pénal Général, Marco Gercke, Germany, § (E)(3).

[228] See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 52.

Likely due to the growing diffusion of personal devices and a global interconnection network,[229] the CoE Convention and the 2005 Framework Decision recognised the limitation to protected systems as an optional condition. The qualification was re-introduced as a necessary element of the core offence in the EU 2013 Directive, essentially narrowing the norm's scope.[230]

This condition requires the unauthorised access to be done bypassing the code-based restriction. It thus excludes liability for mere breaches of the will of the *dominus loci,* such as remaining in a computer system, or exceeding a previous authorisation to access.[231] In such cases, the perpetrator does not infringe any security measure.

In the Italian system it is merely required for the computer system to be protected by security measures, while the infringement of these measures is irrelevant.[232] As pointed out by the Italian Supreme Court, the pivotal element of the offence is the *ius excludendi alios* of the *dominus loci.* Security measures are only to be intended as the explicit manifestation of the will of the *dominus* to exclude others.[233] The core element of the norm is thus determined by the presence of a protective system, and the breach of such system becomes extraneous.[234]

Inter alia, Austria (§ 118a *Strafgesetzbuch*) and the Netherlands (Art. 138a) require a breach of security measures. Romanian Law 161/2003 considers infringing a security measure as an aggravating circumstance of the basic provision (greatly increasing the punishment, from imprisonment from 6 months to 3 years and a fine, to imprisonment from 3 to 12 years).

---

[229] See EU, *Proposal for a Council Framework Decision on attacks against information systems* (n 112), 12 "it is an unfortunate fact that a high proportion of users leave themselves exposed to attacks by not having adequate (or even any) technical protection".

[230] Instead, it was completely excluded from the EU, *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, SEC(2010) 1122 final, SEC(2010) 1123 final, COM/2010/0517 final, COD 2010/0273.

[231] See O. S. Kerr, 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes' (n 208), 1599 – 1600.

[232] A similar approach was endorsed by the EU, *Proposal for a Council Framework Decision on attacks against information systems* (n 112).

[233] ITA, Corte di cassazione, *Judgment n. 12732, 7 November 2000*.

[234] An analogous position was provided by the old version of §202a German Criminal Code. The most recent formulation requires the actual infringement of the protections.

The meaning of "security measures"[235] – which could be interpreted to refer to both physical (e.g. a closed entrance to the computer room) and electronic (e.g. a firewall) measures –[236] is usually not explicated in the statutes and is left to the interpreter to define.[237]

...generating damages.

The generation of damages by the act is a critical qualitative element of the offence. Since it requires an actual harm to the integrity of computer systems and data, it considerably postpone the stage in which liability is activated. Furthermore, it partially merges illegal access with the offences of data and computer interference.[238]

The Commonwealth of Independent States Agreement is the only binding international instrument which envisages such an element. Article 3.1.a requires the Parties to criminalise "the illegal accessing of computer information protected by the law, where such act results in the destruction, blocking, modification or copying of information or in the disruption of the functioning of the computer, the computer system or related networks".

Neither the CoE Convention nor the EU instruments on cyberattacks provide for this qualification. The Czech Republic is the only European State whose illegal access offence requires damage to data. However, the Report on the implementation of the EU Framework Decision found the Czech solution to be irreconcilable with the EU obligation.[239]

In some systems (such as Italy and France), and in the League of Arab States (LAS) Convention,[240] this condition is considered as an aggravating circumstance, offering a scaled punishment when effective damages have been produced.

---

[235] The formulation in the international instruments, and in most national legislations, is in a plural form. This hardly signifies, however, that the existence of a single security measure, such as a password, is to exclude the applicability of the norm.

[236] See, *inter alia*, S. Portesi, 'Attacks against information systems: an analysis of aspects related to illegal access', (2004) 5 Ciberspazio e diritto 411, 428.

[237] Cfr Romania, *Law 161/2003*, art 35.1.h.

[238] See *infra* § II.IV.II-III.

[239] See EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 4.

[240] LAS, *Arab Convention on Combating Information Technology Offences* (2010), Article 6.

The mental element.

Dolus…

All the multilateral instruments on cybercrime require the offence to be committed intentionally. As pointed out in the Explanatory Report on the CoE Convention, the exact meaning of the term is left to each State party.[241] However, at the national level, *dolus eventualis* is usually excluded.[242]

According to the correspondence principle, the state of mind of the agent is required to cover all of the constitutive elements of the norm. Therefore, it necessarily affects the scope of possible qualitative conditions attached to the core offence. In particular, problems may stem from the requirement of a security measure protecting the system.[243] When such an element is not accompanied by the requirement of an actual infringement of the protection, the perpetrator's lack of knowledge of the existence of the protection (for instance, in cases the security measure is inactive, or does not cover the "entrance" through which the system is accessed) may exclude liability.

…and further intent / knowledge?

The requirement of a further intent is of particular importance, since it may direct the norm's scope to behaviours which concretely endanger the protected legal interests.

It is envisaged by the CoE Convention as an optional element of the offence. [244] At the EU level, neither the 2005 Framework Decision nor the 2013 Directive contains it. A further intent to cause damage to a natural or legal person, or to result in an economic benefit was only envisaged by the 2002 Proposal as an alternative necessary requirement of the offence together with the element of the presence of specific protective measures.

In some systems, a further intent may be the element of an aggravating circumstance (e.g. in the Romanian system: intent to obtain computer data)[245], or characterising a separate offence (e.g. in the UK system "unauthorised access with intent to commit or facilitate commission of further offences")[246].

---

241 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 39.

242 See UNODC, *Comprehensive Study on Cybercrime* (n 66), 84.

243 See I. Salvadori, 'L'accesso abusivo ad un sistema informatico o telematico" (n. 138), 137.

244 See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 53; See also OECD, *Report ICCP n. 10, Computer-related Crime: Analysis of Legal Policy* (1986), 70.

245 Romania, *Law 161/2003*, Article 42(2).

246 UK, *1990 Computer Misuse Act*, Section 2.

The formulation of such specific intent varies considerably. The CoE Convention adopted a formulation "of obtaining computer data or other dishonest intent". A "fraudulent" intent is envisaged by two non-European multilateral instruments,[247] and at the domestic level, by the French system.[248] However, in the latter case, the specific intent does not cover a harmful intention, and it is substantially restricted to the knowledge of the irregularity of their act,[249] which can materialise by the simple violation of a security measure.[250] A similar approach is provided for in the UK system – where the offence requires that the perpetrator "knows at the time when he causes the computer to perform the function that that [the unauthorised character] is the case"[251] – or in the Belgian system ("*sachant qu'il n'y est pas autorisé*")[252].

The Austrian basic offence of illegal access requires intent to obtain data without right for oneself or for another unauthorised person, to make it available to another person for whom it is not destined, to use it or to make it public, and to procure in this way an economic gain for oneself or another person or cause a disadvantage to another person.[253] The Austrian solution thus follows the option envisaged by the CoE Convention provision. However, it was considered irreconcilable with the Framework Decision's obligations by the 2008 Report on the implementation of the 2005 Framework Decision.[254] The Report thus shows a conflict between the obligations stemming from the EU and CoE instruments on cybercrime.

---

247 African Union, *Convention on Cyber Security and Personal Data Protection*, Art. 29 (1), although interestingly, the adverb is used only with regard to the offence of illegally remaining (lett. c), and illegal access to data contained in a computer system (lett. e); Economic Community of West African States, *Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS* (n 220), 5.

248 FR, *Code Pénal*, Article 323-1.

249 See A. Lepage, P. Maistre du Chambon and R. Salomon, *Droit Penal des Affaires* (LexisNexis 2015), 254; FR, Cour d'Appel de Paris, 15.12.1999: D. 2000, inf rap p 44.

250 See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 15.

251 UK, *1990 Computer Misuse Act*, Section 1 (1) (c).

252 Belgium, *Code Pénal / Wetboek van Strafrecht*, Article 550bis (knowing that it is not authorised).

253 Austria, *Strafgesetzbuch,* Article 118a; Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Colloque Préparatoire Section II. Moscou (Russie), 24-27 avril. 2013, Droit Pénal Partie Spéciale, Madalena Pampalk, Austria, 2.

254 EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 4.

"At least in cases which are not minor": closing condition and the Report on the Implementation…

The illegal access provision contained in the EU instruments on cybercrime substantially echoes the core offence delineated in the CoE 1989 Recommendation and in the Budapest Convention. Contrary to the Proposal, the only qualitative condition envisaged for the offence is the infringement of a security measure. Nonetheless, the EU instruments provide for a closing condition of exclusion of liability for minor cases.

The 2008 Report on the implementation of the 2005 Framework Decision, based on Article 12 of the Framework Decision, is particularly useful to understand the exact scope of the closing condition.[255]

The Report considered that State Members[256] "have incorporated the main obligation, i.e. to ensure that intentional access without right to the whole or any part of an information system is punishable as a criminal offence"[257]. Yet, even at the time of the Report, the actual scope of the domestic provisions under examination varied considerably. *De facto*, some of them could be considered as providing a narrower protection than the one delineated by the Framework Decision. Although not censured by the Report, it is unlikely that these cases fall under the scope of the closing condition.

The Report found that four systems had not correctly implemented the obligation stemming from Art. 2. However, it specified that their divergences did not correspond to "cases which are not minor". Aside from the two afore-mentioned cases, i.e. Austria and the Czech Republic, the Report found that the Latvian norm – criminalising only access causing "substantial injury" – and the Finnish provision – criminalising access which substantially "endanger" data – do not comply with the Framework Decision. According to the Report, such provisions are posing "a serious risk to the objective to approximate Member State rules on criminal law in the area of attacks against information systems"[258]. However, the Austrian offence appears in line with the EU norm, as presented in the Proposal. The Finnish provision is consistent with the aim of protecting data security at an early stage. Moreover, the same qualitative restriction may be easily reached by a system that requires – in order for liability to arise – the actual harm or endangerment of the legal interest protected (namely, in systems that put an emphasis on the *Rechtsgut* concept).[259]

---

[255] The Report on the implementation of the Directive, conversely, do not contain such a detailed analysis.

[256] At least, the 20 States that have complied with their duty, deriving from Art. 12 Framework Decision, to notify the concrete implementation to the General Secretariat of the Council and to the Commission.

[257] See EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 4.

[258] *Ibid.*

[259] See *infra* n 425.

Possibly, the results of the Report could be related to the legal interest protected by the norm. The Report specifies that the core interest protected by Art. 2 of the Framework Decision is the confidentiality of information systems. This interpretation provides a more precise scope to the norm, embracing some national approaches (such as those of Germany, Spain, and Italy) and excluding others (such as the Finnish) that are focused on data integrity. However, it contradicts the traditional approach to the offence, as expressed in the CoE instrument, aimed at protecting the general security of computer systems and data (thus setting liability at an earlier stage than provisions requiring harm to confidentiality of data). Such an interpretation may create a substantial divergence between the CoE Convention and the EU obligations, notwithstanding their similar formulation.

In any case, the Report notes that the meaning of the syntagma "cases which are not minor" requires further specification. It does provide for a rather tautological interpretation of this expression, which is reiterated in the 2013 Directive: "instances […] of minor importance or […] infringement of information system confidentiality […] of minor degree".

…and *de minimis non curat lex*?

Undeniably, the EU instruments seek to avoid overcriminalisation, and in particular criminalisation of "*minor*" offences or border conducts by right-holders and authorised persons.[260] In this regard, the 2010 Directive Proposal stated that: "The Directive contains (…) a provision allowing to criminalise only 'cases which are not minor' in the process of transposition of the directive into national law. This element of flexibility is intended to allow Member States not to cover cases that would *in abstracto* be covered by the basic definition but are considered not to harm the protected legal interest, e.g. in particular acts by young people who attempt to prove their expertise in information technology. This possibility to limit the scope of criminalisation should not however lead to the introduction of additional constitutive elements of offences beyond those that are already included in the Directive, because this would lead to the situation that only offences committed with the presence of aggravating circumstances are covered. In the process of transposition, Member States should refrain in particular from adding additional constitutive

[260] See P. Van De Velde, 'EU Council takes action against attacks on information systems', (2005) Bird & Bird, 2, <http://www.twobirds.com/en/news/articles/2005/eu-council-takes-action-against-attacks-on-information-systems, at 12>.

elements to the basic offences such as e.g. a special intention to derive illicit proceeds from crime or the presence of a specific effect such as causing a considerable damage."[261]

States are thus barred from using additional constitutive elements to exclude criminalisation of trivial offences. *De facto*, the closing condition seems to suggest the use of judicial interpretation or existing substantive and procedural doctrines that permit States to avoid or discontinue the prosecution of trivial offences (particularly in cases of a low degree of harm or endangerment to the protected legal interest).[262]

Furthermore, the condition recommends avoiding the criminalisation of acts not harming or endangering the protected legal interest. However, it does not give sufficient guidance on the exact nature of such interest. The example used ("acts by young people who attempt to prove their expertise in information technology") is, in any case, falling under the theoretical scope of most national provisions on illegal access.[263]

Criminal policy-oriented institutes, such as those focused on discretionary prosecution, may allow for the criminalisation of conducts that *in concreto* fall under a cyber offence, but generate a positive outcome to society, to be excluded. The necessary balance between positive and negative outcomes of an act could be difficult to regulate within a positive norm. However, such regulation can be outsourced to prosecution policies. A clear example of acts meeting a sufficient threshold of "positivity" to exclude criminalisation is the cyberattacks by hacktivist groups against terrorists. In its "cyberwar" against ISIS[264], the hacktivist group Anonymous routinely violated cybercrime provisions. However, no prosecution has ever been initiated, nor is it to be expected that any will be

---

[261] EU, *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA* (n 230), 7.

[262] Indeed, this also depends on whether a State envisages a mandatory or discretionary system of prosecution (although even in the former systems some exceptions to compulsory prosecution exist). See, for instance, ITA, *Codice Penale*, Art. 131-bis c.p. "Esclusione della punibilità per particolare tenuità del fatto" (C. F. Grosso, 'La non punibilità per particolare tenuità del fatto' (2015) Diritto Penale e Processo, 517); UK, *The Code for Crown Prosecutors,* issued by the Director of Public Prosecutions (DPP) under section 10 of the Prosecution of Offences Act 1985 (2018), § 3.4: "Prosecutors should (…) swiftly stop cases which do not meet the evidential stage of the Full Code Test (see section 4) and which cannot be strengthened by further investigation, or where the public interest clearly does not require a prosecution", and §4.12, http://www.cps.gov.uk/publications/docs/code_2013_accessible_english.pdf. See also US, *Model Penal Code,* §2.12 (2) De Minimis Infractions: "The Court shall dismiss a prosecution if, having regard to the nature of the conduct charged to constitute an offense and the nature of the attendant circumstances, it finds that the defendant's conduct: (2) did not actually cause or threaten the harm or evil sought to be prevented by the law defining the offense or did so only to an extent too trivial to warrant the condemnation of conviction".

[263] See, for instance, ITA, Tribunale di Catania, Ufficio del Giudice per le Indagini Preliminari, Decreto di archiviazione, 15 luglio 2019, recognising that "ethical hacking" cannot be considered as illegal access to a computer system. See also *infra,* n 198.

[264] See, *inter alia*, J. Shammas, 'Anonymous hacker reveals how they will destroy ISIS and its ability to carry out terror attacks' (The Mirror, 1 December 2015) <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-693133.1>.

in the future.[265] Nonetheless, no traditional criminal law doctrine may justify such acts.[266] If the "justification" of the act is therefore to be found in a policy decision to not enforce the law, such decisions are related to the positive outcome of a given act – in its moral value. In the case of Anonymous's attacks against ISIS, the reason for their non-prosecution seems to be rooted in a sort of a "criminal law of the enemy"[267]. The application of this, however, seems to have extended beyond that of the traditional doctrine, justifying the use of public (digital) force by private citizens.

---

[265] See J. O'Connel, 'Stanford Scholar: Us Unlikely to Prosecute Anonymous for Harassing Isis' (Hacked, 24 November 2015) <https://hacked.com/stanford-scholar-us-unlikely-prosecute-anonymous-harassing-isis/>.

[266] For instance, it is hard to subsume the attack under the self-defence or defence of others justifications: there is no logical, temporal or physical connection between the act and the response.

[267] See G. Jakobs, Kriminalisierung im Vorfeld einer Rechtsgutsverletzung', in *Zeitschrift für die gesamte Strafrechtswissenschaft* (De Gruyter 1985).

II.IV. THE OTHER CYBER OFFENCES *STRICTO SENSU*.

The offence of illegal access to computer systems epitomise the characteristic and problematic aspects related to the criminalisation of cybercrime conducts. The analysis of the other cyber offences *stricto sensu* will thus focus on their main specific aspects, with particular attention paid to the impact of the international instruments on domestic systems.

II.IV.I. ILLEGAL INTERCEPTION OF COMPUTER DATA.

The enactment of an offence of illegal interception, covering acts of computer and data espionage, was initially recommended in 1989 by the CoE Committee. The aim of such an offence was to overcome the problems related to the use of non-specific provisions on data espionage (such as interception of oral communications[268] or theft).[269] The CoE Recommendation, in its accompanying report, stated that: "interception […] relates to 'listening' to the content of communications, to the procuring of the content of data either directly, through access and use of computer system, or indirectly, through the use of electronic eavesdropping or tapping devices"[270]. The offence was essentially repeated – with some minor departures – in Art. 3 of the Budapest Convention and again in the 2013 EU Directive. *Per contra*, the 2005 EU Framework Decision did not contain an analogous provision.

The legal interest protected, and its relationship with illegal access.

The offence of illegal interception is aimed at protecting the confidentiality of computer data and systems. It focuses on the right to privacy of electronic communication,[271] while, at the same time, protecting the correctness of data transfer processes.[272]

---

[268] For instance, applied on data interception in Germany till 2007, when Section 202b *Strafgesetzbuch* was introduced.

[269] See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 53; UNODC, *Comprehensive Study on Cybercrime* (n 66), 86.

[270] *Id.* See also CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 53.

[271] CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §51.

[272] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 17.

The scope of this offence is narrower than that of illegal access. However, as previously pointed out, in some legal orders – where illegal access is oriented towards the protection of the confidentiality of computer systems and data – the two offences may move closer, or even overlap. [273] In the German system, Section 202b *Strafgesetzbuch* on illegal interception of data (introduced in 2007)[274] is almost identical to §202a on illegal access. The only element of specialisation of the former is that data is illegally obtained from non-public transmissions or electromagnetic emissions. The relationship between the offences of illegal access and illegal interception will therefore be regulated by the *lex specialis* principle.[275]

According to the definition contained in the CoE and EU instruments on cybercrime, the target of the illegal interception is the "transmission" of computer data "to, from or within a computer system"[276]. A contact point between illegal interception and illegal access is interception "within" a computer system, thus between technical components of a computer system ("direct" interception of data). In such a case, the *discrimen* between the two norms is the static or dynamic nature of data: i.e. whether data is stationary within the hardware of a computer system, or else moving between its various components.

The material element.

The interception without rights of non-public transmissions and electromagnetic emissions…

The offence covers the interception of data in the transfer process, which is recognised as vulnerable and therefore in need of specific protection. Most of the multilateral cybercrime instruments limit the object of interception to the non-public transmission of data.[277] The CoE Convention and the 2013 Directive include "electromagnetic emissions", offering a broader scope to the offence.

The term "non-public" is intended to qualify the nature of the transmission process. It does not refer to the nature of the transmitted data. The public transmission of data in any form is therefore

---

[273] In the Spanish system, for instance, the two offences are part of the same article. Spain, *Código Penal*, Article 197 (1): "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."

[274] Before 2007, illegal interception was covered by the section 201 *Strafgesetzbuch* on the violation of confidentiality of the spoken words.

[275] See G. Jakobs, 'Die kunkurrentz', in *Strafrecht, allgemeiner Teil: die Grundlagen und die Zurechnungslehre* (De Gruyter 1993), 861ff.

[276] CoE, *Convention on Cybercrime* (n 81), Art. 3.

[277] Cfr LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Art. 7: "interception of the movement of data".

excluded from the scope of the norm. Private forms of transmission through public channels are included.[278] However, the distinction between public and non-public transmission is not widely followed in national legislations, which usually adopt broader formulations, such as the Portuguese provision, which covers "all communication within a computer system".[279]
The syntagma "without right" is evidently aimed at excluding surveillance authorised in the context of intelligence or criminal investigations.

...by technical means.
The CoE Convention and the 2013 EU Directive require the act of interception to be committed using technical means. This requirement had already been envisaged by the 1989 CoE Report which highlighted its role as a restrictive element avoiding overcriminalisation.[280]
Generally, the analysis of domestic legislations demonstrates a tendency to provide broad protection to the confidentiality of data. For instance, neither France nor Italy limit the scope of the offence to non-public transmission. Furthermore, the Italian norm covers "communications" and "all remote transmission of sounds, images or other data".[281] Neither system requires the interception to be committed by technological means. Moreover, they extend the offence's conduct to: acts of "diversion, use and disclosure" of communication and "installation of devices to intercept communication"[282] (France); "obstruction and interruption", "falsification, alteration and suppression" of communication and "installation of devices to intercept, obstruct or interrupt communication" (Italy)[283].

The mental element.

Both the CoE Convention and the EU 2013 Directive require the offence to be committed "intentionally". The Budapest Convention envisages an additional condition of a further "dishonest

---

278 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 54.

279 See Portugal, *Law 109/91* (n 149), Art. 8.

280 See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 54. See also CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 53.

281 ITA, *Codice Penale*, Artt. 617quater – 623bis. The French criminal code, on the other hand, limits the scope of the norm to "correspondences sent, transmitted or received by means of telecommunications". FR, *Code pénal*, Art. 226-15.

282 FR, *Code pénal*, Art. 226-15

283 ITA, *Codice Penale*, Artt. 617 quater- quinquies – sexies.

intent",[284] which is adopted by few domestic jurisdictions[285] (e.g. the French system requires a "malicious intent") [286]. The EU Directive does not envisage any similar qualifying condition.

II.IV.II. DATA INTERFERENCE.

Originally, the offence of data interference was aimed at protecting computer data in a similar way as physical goods are protected from being damaged.[287] The 1989 CoE Recommendation envisaged an offence of "damage to computer data", whose *actus reus* was the "alteration, erasure, suppression of computer data or computer programs". The offence was reiterated in the CoE Convention under the name of "data interference", with a slight variation of the terms indicating the required material elements. Importantly, the Convention envisaged a possible limitation of the scope of criminalisation to acts generating "serious harm". The Convention's provision was repeated almost *verbatim* in the EU instruments, which added the conduct of "rendering (data) inaccessible".[288]

The legal interests protected.

The offence of data interference is aimed at protecting the integrity and the availability of data. As pointed out by the 1989 CoE Report, such a protection contains both quantitative and qualitative aspects. [289] Quantitatively, it protects data in their "physical" integrity. Qualitatively, it protects data in their capacity to function. Due to the functional nature of data, any alteration of their "quality" may hinder its availability.

Before the enactment of cyber-specific offences on data interference, States tended to subsume damage to data under traditional damage offences. This approach, identifying data as "goods", led to a series of problems. It restricted the aim of the norm, focusing mostly on protection of data's

---

[284] See supra, on the specific intent of illegal access. Interestingly, the Explanatory Report recognises the close relation existing between illegal access and illegal interception in some State parties. It suggests modulating the two offences according to the same mental element, in case the domestic provision on illegal access requires a further dishonest intent. CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 59.

[285] UNODC, *Comprehensive Study on Cybercrime* (n 66), 88.

[286] FR, *Code pénal*, Art. 226-15 "commis de mauvaise foi".

[287] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 60.

[288] However, the EU, *Proposal for a Council Framework Decision on attacks against information systems* (n 112), was not envisaging a separate offence of data interference, incorporating it under the provision on illegal interference with information systems, with which the former offence have a strong relationship..

[289] See CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 44.

quantitative integrity.[290] Moreover, it excluded data lacking economic value, but still worthy of protection (for instance, data that have a pivotal position in the overall functioning of the system, or that relate to the private sphere).[291]

A further problem related to the immaterial nature of data.[292] In the UK system, in a series of cases anterior to the enactment of the 1990 Computer Misuse Act, damage to data was handled under the 1971 Criminal Damage Act. That act stated that "a person who without lawful excuse destroys or damages any *physical* property belonging to another intending to destroy or damage such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence."[293] In the Italian system, these behaviours were treated through Article 635 of the *Codice Penale* on the traditional damaging of physical goods. In both systems, liability was not based on damage caused to data itself – which, not being "material" or "tangible", was not covered by the norm. Rather, liability was based on the related alteration of the material parts of the hardware, or its functioning. [294] Mere alteration of data that do not have a "material" effect on hardware was left uncovered.

Interestingly, before the enactment of a specific offence, the UK system attempted to subsume illegal access under the offence of abstraction of electricity.[295] In the Italian system, the provisions on theft – the object of which includes "electrical energy and other energy of economic value" – were used as a basis for a doctrinal consideration on the possible extension of the concept of *res* to cover digital data.[296]

---

[290] *Ibid.*

[291] *Ibid.*

[292] See also U. Sieber, 'Mastering Complexity in Global Cyberspace' (n 7).

[293] Italics added.

[294] See ITA, Cassazione Penale, *Judgment n. 1282, 9.10.1996*; UK, *Cox v Riley*, [1986] 83 Cr App R 54, DC; UK, *R v Whiteley*, [1991] 93 Cr App R 25, CA.

[295] See D. I. Bainbridge, 'Hacking - The Unauthorised Access of Computer Systems: The Legal Implications' (1989) 52 The Modern Law Review, 240. Interestingly, even the offence of "theft of electricity" was created in order to overcome the problems related to applying traditional theft provisions to electric energy. In this regard, many States perceived problems in relation to the *lex certa* principle. In some cases, these problems eventually led to the enactment of new theft provisions aimed at covering electric energy. In other cases, the issue was resolved via interpretation. In the Dutch system, the Dutch courts interpreted the term "good" ("*enig goed*") in Article 310 of the Criminal Code as encompassing electricity. The argumentation used was that "goods" have an autonomous existence, availability, capability to move and economic value: thus electricity, possessing such qualities, pertains to this category. Importantly, according to the court, such an interpretation was consistent with the modernisation of life. Similar interpretations have been conducted with regards to electronic data. See M.S. Groenhuijsen and F.P.E. Wiemans, *Van electriciteit naar computercriminaliteit* (Gouda Quint 1989), 84.

[296] See L. Leone, 'Il nuovo danneggiamento informatico', (2010) 1 Ciberspazio e diritto, 212. It shall be highlighted that, in a such case, the extension could have been tied to the typical limitation of traditional damage offences to the protection of economic property, which might be improper with regards to data.

Some States still do not envisage a specific offence of data or system interference and maintain the use of traditional damage offences. In the Danish system, data damage is covered by Section 291 of the Danish criminal code, which punishes "any person who destroys, damages, or removes objects belonging to others". The inclusion of electronic data under the scope of the norm was endorsed through an extended judicial interpretation of "objects" to cover immaterial data.[297] Under scrutiny in the 2008 Report on the Implementation of the EU Framework Decision, the Danish approach gave rise to uncertainties about its full compliance with the obligations stemming from the EU instrument.[298]

The material element.

Altering, erasing, suppressing, damaging, deleting, deteriorating data…

Various conducts can damage data, harming their integrity and availability. They all involve data alteration, through their complete deletion, modification, or suppression (their being rendered non-existent or unusable). The CoE Convention gives examples of a series of conducts leading to data alteration. Some domestic provisions present a similar terminology to that of the international instruments. Other systems have preferred the generic term "alteration".[299]

Data are protected regardless of whether they are stored, processed or transmitted.[300] As previously mentioned, the Italian system affords specific protection against the alteration of data during its transmission. However, the Italian provision is specifically aimed at protecting the authenticity of transmissions, in order to tackle computer forgery.

The French system provides for a narrower scope of protection, limited to data contained in an automated data processing system. This approach moves the scope of the norm closer to the offence of system interference. At the same time, it may leave uncovered data located outside the processing system (e.g. in a USB drive).[301]

…without rights…

As pointed out in the 1989 CoE Report, and in the Explanatory Report to the Budapest Convention, the syntagma "without rights" is of critical importance. It excludes any "common

---

[297] DK, Eastern High Court, *U 1987.216.*

[298] EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 6.

[299] …which, thanks to judicial interpretation, can easily cover all the above-mentioned conducts.

[300] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 62.

[301] FR, *Code Pénal*, Art. 323-2.

activity inherent in the design of network or common operating or commercial practice", such as the reconfiguration of a system due to software updates or the modification of data for anonymous communication (encryption).[302]

Due to an enduring relation between the cyber-specific and the traditional offence of criminal damage, many domestic provisions retain in the former the traditional element requiring that the material object of the crime "belongs to others". This is the case in the Italian and Croatian systems.[303]

However, this element is related to the traditional notion of property rights held in respect to tangible goods. It may not entirely fit a lack of authority or entitlement to act over data. Furthermore, this element may exclude from the scope of the norm the modification of owned data that negatively affects the qualitative integrity or availability of other data, linked to those that are modified.

…if it results in serious harm (and excluded cases which are minor).

Both the CoE Convention and the EU instruments provide for a possible exclusion of liability in minor cases. This particular attention to a *de minimis* approach is common to all the offences envisaged by the EU instruments on attacks against information systems. Conversely, in the CoE Convention it covers only Article 4 on data interference (as an optional condition), and Article 5 on system interference (enclosed in the core norm).[304]

The Report on the implementation of the EU 2005 Framework Decision mentions three cases in which the said closing condition would apply. The Czech provision – requiring intent to cause harm or loss – and the Estonian provision – requiring that significant damage is caused – were considered to be consonant with the EU obligations.[305] It could thereby be inferred that the EU closing condition does encompass the CoE element of serious harm.

Conversely, the Latvian provision – requiring that "protective systems are damaged or destroyed thereby or substantial harm has been caused thereby" [306] – was found by the Commission not to

---

[302] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 62. According to the 1989 CoE Report (*supra* n 60) this element played an analogous role of the element of "belonging to another person" in the traditional offence of damaging property (thus being related to the property rights on data damaged); provided that "the notion of property in corporeal goods is not applicable to data".

[303] ITA, *Codice Penale*, Art. 635bis; Croatia, *Penal Code*, Art. 223(3).

[304] With regard to data interference, this criterion is left to national interpretation. Parties making use of it shall notify the Secretary General. See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §64.

[305] EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), § 2.5.

[306] Latvia, *Criminal Code*, Art. 243.

properly comply with the international provision. Currently, the Latvian norm has not been amended. *Per contra*, the Czech "intention of causing damage" and the Estonian requirement of "significant damage" have moved from being a necessary element (thus defining the limit of criminalisation), to becoming an aggravating circumstance of the basic offence (thus extending the scope of the norm).[307]

The mental element.

The CoE and the EU cybercrime instruments require the act of interference with data to be committed "intentionally". However, some domestic systems widen the scope of the provision to cover reckless conduct. Criminalisation on the basis of recklessness is also envisaged by the Commonwealth Model Law on Cybercrime.[308] It should be considered that – due to the peculiar vulnerability of data, which are "intangible and rather volatile" and "easier to change or delete accidentally than (...) physical objects"[309] – an extension of the required mental state to cover reckless conducts significantly extends the scope of the offence of data interference, opening up the risk of overcriminalisation.

In line with the traditional offences around criminal damage, the Dutch provision even covers culpable conducts (but in such a case requires a material element of "serious damage").[310]

II.IV.III. SYSTEM INTERFERENCE.

The offence of system interference (referred to in the 1989 CoE Recommendation as "computer sabotage") aims at criminalising the intentional hindering of computer systems by using or influencing computer data.[311] The two offences of system interference and data interference are strongly related, as the latter could be an antecedent of the former. At the international level, both the CoE Convention and the EU instruments on attacks against information systems envisage separate provisions for the two offences. Conversely, the LAS Convention combines the two offences

---

[307] Estonia, *Criminal Code*, Art. 206; Czech Republic, *Criminal Code*, Art. 230.

[308] The Commonwealth, *Model Law on Computer and Computer Related Crime* (n 74), Art. 6.

[309] See P. De Hert, G. González Fuster and B. Koops, 'Fighting cybercrime in the two Europes. The added value of the EU Framework Decision and the Council of Europe Convention' (n 163), 508.

[310] NL, *Wetboek van Strafrecht*, Art. 350b. The mental element is '*schuld*' (culpa).

[311] CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 65.

into a single provision. A similar approach was followed in the 2002 Framework Decision Proposal and can be found in certain domestic systems.[312]

The legal interests protected.

This offence is aimed at protecting the integrity and availability of computer systems. The qualitative aspect of such protection, already examined with regard to data interference, here acquires a specific significance. This norm is chiefly intended to offer protection to digital systems from qualitative interference with their functioning. On this point, the 1989 CoE Report stated that: "disturbances in computer and telecommunications systems may have even more negative consequences than mere negative alterations of computer data and programs. Because of the increasing dependence of modern society on these systems, they play such an important role that the protection of the functioning of the system is of great interest not only to the owners/users of them, but in many cases also to the public".[313]

With the exponential evolution of societal reliance on technology, such considerations have grown in importance and in normative relevance.

The legal interest protected by the offence of system interference is the proper functioning of a computer system or network. However, an increasing amount of diverse interests depends on the correct functioning of computer systems. In particular, in case of cyberattacks against critical digital infrastructures, the integrity and availability of those systems may be intimately connected to other vital public interests.

The material element.

The serious hindering of the functioning of a computer system (without right)…

The core element of the crime is the result of a hindrance of the functioning of a computer system. The term "hindering", used in the CoE Convention provision, refers to any "interference" with the proper functioning of a system.[314] The EU instruments further specify the formulation, adding to the *actus reus* the "interruption" of the functioning of a computer system.

Both the CoE Convention and the EU instruments adopt a qualitative threshold activating criminal liability. According to such instruments, the event of hindrance or interruption must be "serious". In

---

[312] See, e.g., Latvia, *Criminal Code*, Section 243.

[313] CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 46.

[314] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §66.

the EU instruments, this *de minimis* approach is further stressed by the final condition of excluding liability in minor cases.[315]

The CoE Convention does not define the threshold of "seriousness", whose exact determination is left to the State Parties. The Explanatory Report, however, provides for a (rather tautological) explanation: "the drafters considered as 'serious' the sending of data to a particular system in such a form, size and frequency that it had detrimental effect on the ability of the owner or operator to use the system, or to communicate with other system".[316] The 2002 Framework Decision Proposal is also of scarce aid in defining the concept. After stating that each Member States "shall determine for itself what criteria must be fulfilled in order for an information system to be considered as 'seriously hindered'", the instrument specifies that "minor nuisances or disruptions in the functioning of the service should not be considered as fulfilling the threshold of seriousness". This explanation seems to merely state the obvious, since "minor" is an antonym of "serious".

Due to the lack of *ex ante* guidance, in order to better appraise the scope of this criteria, it may be helpful to consider the Report on the implementation of the 2005 Framework Decision. The Report clearly considered both the Latvian approach – criminalising acts of system interference only where "protective systems are damaged or destroyed or losses [are] caused on large scale" – and the German approach – criminalising interference only with computer systems "of substantial importance to others" – to be inconsistent with the obligation of Art. 3 of the Framework Decision.[317] However, the Report limits its analysis to the "law in the books", with no examination made of the domestic judicial interpretation of the terminology used in the national systems.[318]

…by "altering" computer data.

According to the CoE Convention and the EU instruments on attacks against information systems, the hindrance to the given system must be realised through data interference. In comparison with the conducts envisaged by its Art. 4 on data interference, Art. 5 of the CoE Convention adds the material element of "inputting and transmitting data." The EU instruments, on the other hand, include the conduct of "rendering such data inaccessible" (which is also contained in the provision on data interference). According to some commentators, the specific attention paid at the EU level to outlining the *actus reus* is indicative of a particular sensitivity towards certain types of cyberattacks

---

315 See *supra* § II.III.I.

316 CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 67.

317 EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 5.

318 Such as "serious" – used, for instance, in the Italian system (IT, *Codice Penale*, Art 635quater) – or "severe" – used in the Austrian system.

of primary empirical importance, such as Denial of Service attacks.[319] Indeed, the German provision on system interference was amended in 2007 to include the conduct of "entering or transmitting data" with the specific aim to cover DoS attacks.

However, while some systems – such as the Italian or Portuguese ones[320] – faithfully reproduce the material scheme of the international provisions, others – such as the French and Croatian systems[321] – do not provide either the requirement of "seriousness" of the result, or the necessary conducts of data interference leading to it. Their scope therefore appears to be substantially broader than that of the international instruments.

Interestingly, some soft-law multilateral instruments include cutting off electricity supply to computers, corrupting a computer system, and generating electromagnetic interference in the *actus reus*.[322]

The mental element.

According to the CoE and EU provisions, the act of interfering with the functioning of a computer system is to be committed intentionally. The *dolus generalis* must cover all the elements of the norm, including the result. The perpetrator must therefore intend to cause a serious hinderance to the system.

Interestingly, in the 1989 CoE Recommendation, the hindrance was required only at the mental stage. The difference between the offences of data and computer interference was thus limited to the intent to hinder the functioning of a computer or a telecommunication system (*dolus specialis*).

Some systems also criminalise acts of reckless interference. As in the case of data interference, the Dutch system even punishes "any person who, through negligence[323], causes any of the property or the infrastructure facilities defined in the preceding section [*inter alia*, computerised device or system or telecommunication infrastructure facilities] to be destroyed, damaged, rendered unusable or defective, or disposed of", with reduced penalties. [324]

---

[319] See L. Picotti, 'Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale' (2005) Diritto dell'Internet, 199.

[320] ITA, *Codice Penale*, Art. 635 quater (introduced in 2008); Portugal, *Law No. 109/2009 of September 15, 2009 (Cybercrime Law)*, Art. 5.

[321] FR, *Code Pénal*, Art. 323-2; Croatia, *Criminal Code*, Art. 223 (2).

[322] The Commonwealth, *Model Law on Computer and Computer Related Crime* (n 74), Art. 7; ITU /CARICOM/ CTU Model Law, supra n. xxx, at Art. 3.

[323] (Schuld). See *supra*, n 310.

[324] NL, *Wetboek van Strafrecht,* Art. 351bis.

II.IV.IV. MISUSE OF DEVICES.

The offence of misuse of devices used (or usable) to commit cybercrime is substantially a cyber-specific transposition of the offence of illicit possession of burglary tools. Its function is to advance the area of criminal liability to acts that do not generate concrete offence to the protected interests, but merely endanger them. It therefore serves an aim of prevention of the crime. Additionally, it aims at combating black markets in which hacking tools are traded.[325]

At the international level, the offence is envisaged in the CoE Convention and in the 2013 EU Directive. According to the Explanatory Report to the CoE Convention, the provision was seen as a middle ground between criminalising the possession of the tools that can be exclusively used for illicit purposes, considered too narrow, and criminalising the possession of every tool that could have a dual licit/illicit use, which was considered too broad. [326]

The material element.

The possession, production, sale, procurement for use, import, distribution, or otherwise making available (without right) of a device.

The core element of the offence is the unauthorised possession, production, sale, procurement for use, import, distribution, or otherwise making available, of a device – including a computer program, a password, an access code, or similar data – aimed at providing access to a computer.

As mentioned above, the drafters of the CoE Convention were aware of the problems related with a broad criminalisation of tools that may have be adaptable for illicit uses. The distinction between licit and illicit conducts is guaranteed by the element of the lack of right ("without right")[327], and by the subjective element. Moreover, in case of the production, sale, procurement for use, import, distribution, or otherwise making available of a device, the provision requires such devices to be designed or adapted *primarily* for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

Notwithstanding the specific attention given to avoiding overcriminalisation (using a qualitative restriction of the offence), the CoE Convention's provision stresses that: "this article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession […] is not for the purpose of committing

---

[325] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 71.

[326] *Id.*, § 73.

[327] *Id.*, § 77.

an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system".

Among the various conducts covered by the international formulations, the catchall term "otherwise making available" was specifically intended to address the online diffusion of tools (for instance, the creation of hyperlinks in order to facilitate access to them).[328] In the absence of specific malicious intent, online diffusion, together with possession, is prone to create the risk of overcriminalisation. Furthermore, it may negatively impact upon the diffusion of technological knowledge.[329]

The CoE Convention allows for reservations aimed to restrict the offence to a core norm of sale, distribution or making available of a computer password or other access data. The EU 2013 Directive, which reprises the formulation of the CoE Convention, does not envisage criminalisation of the possession of tools. At the national level, several domestic provisions restrict the offence to some of the acts enlisted in the CoE and EU instruments.[330]

The mental element.

According to the international provisions, the actor must possess the specific intent of committing offences against the confidentiality, integrity, and availability of computer systems or data. This element is of paramount importance in carving out the scope of the norm in a way that avoids overcriminalisation. However, several national provisions do not envisage such additional further intent.

The German system – at section 202c *Strafgesetzbuch*, introduced in 2007 – criminalises preparatory acts to an offence of data espionage, interception of data and – according to § 303 (a) and (b) – of data or system interference. In the German provisions, the tool in question must be designed or adapted to allow access to data. This requirement is sufficient to show the aim of committing the above-mentioned offences,[331] and substantially hypostatise the specific intent of the CoE and EU provisions. However, the scope here is broader, since the mere possession or dissemination of a so designed or adapted tool, notwithstanding its possible dual-use, is covered by the norm.

The French provision – Art. 323-3-1 *Code Pénal* – does not provide for any specific intent. The syntagma "*sans motif légitime*" (without a legitimate reason) is the only element that may avoid

---

328 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 72.

329 See, for example, World Information Technology and Services Alliance, *Statement on the Council of Europe Draft Convention on Cyber-Crime* (2000) <www.witsa.org/papers/COEstmt.pdf>; 'Industry group still concerned about draft Cybercrime Convention' (Out-Law 5 December 2000) <www.out-law.com/page-1217>.

330 See, for instance, UK, *Computer Misuse Act 1990*, § 3A: "makes, adapts, supplies or offers to supply".

331 See Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), National Report on Germany, Section I, 15-16.

criminalisation. Its scope was clarified in 2013, when the French legislator added "*nomment de recherce ou de sécurité informatique*" (such as scientific research or cybersecurity) to the element. This amendment shows a similar concern to that of Paragraph 2, Article 6 of the CoE Convention. However, it appears of scarce practical use in the application of the norm.[332]

The Italian Criminal Code contains two different provisions on the misuse of devices. Article 615 *quinquies* covers the misuse of devices aimed at committing acts of data and system interference and requires the special intent to commit such crimes. Article 615 *quater* covers possession and diffusion of tools aimed at permitting access to computer systems. In such a case, the perpetrator must have the special intent to gain a financial advantage or to damage a third person via the act. It is interesting to note that the offence of illegal access does not envisage any similar mental element.

The CoE Convention permits States parties to limit criminal liability to possession of a certain number of items (the amount is left to the domestic decision). The Explanatory Report suggests – although using an indicative verbal form – that the number of items may prove criminal intent.[333]

---

[332] See A. Lepage, P. Maistre du Chambon and R. Salomon, *Droit Penal des Affaires* (n 249), 264.

[333] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 75.

II.V. POLITICALLY MOTIVATED DENIAL OF SERVICE ATTACKS: BETWEEN DIGITAL PROTEST AND CYBERCRIME.

The previous subchapter completed the legal analysis of the cyber offences *stricto sensu,* and their constituent elements. This section will deal with a specific type of cyberattack: Denial of Service (DoS) attacks. DoS attacks are among the most common types of cyberattack and are often used as an "electronic" form of protest. The following analysis will show how the existing substantive framework addresses this specific cyber conduct, at the same time taking (or failing to take) into consideration the human rights possibly involved.

A Denial of Service attack can be defined as an attempt to make an online service unavailable by overwhelming it with data. The idea behind it can be easily explained via a simile with a non-digital situation. A man would like to purchase a cake (receive a service). When approaching the bakery, he stumbles in a huge line of people queuing outside. These individuals are not interested in receiving the service. Instead, once they reach the counter, they simply ask for information, and then leave. The bakery (playing the role of the Information Technology Company) cannot handle all the requests coming from fake customers (which results in data flooding) and is therefore unable to serve the real ones. As a consequence, the man is prevented from buying the cake, and service is denied.

DoS attacks first appeared in the 1990s. Over the years, they have constantly increased in number, volume and intensity.[334] They are one of the most used and effective form of cyberattack. On a daily basis, they target a wide range of private and public resources, from banks to government websites.[335] Most of the fame and fortune attributed to DoS attacks derives from their "democratic" nature. They do not require major technical expertise or costly technological equipment.[336]

---

[334] See, inter alia, Akamai, *State of the Internet Security Q4 2015 Report* (Akamai, 2016) <https://www.akamai.com/us/en/multimedia/documents/report/q4-2015-state-of-the-internet-security-report.pdf>; 'DDOS Trends to Watch for in 2020' (EC-Council, 19 December 2019) < https://blog.eccouncil.org/ddos-trends-to-watch-for-in-2020/>.

[335] See also cyber attacks maps available at: http://www.digitalattackmap.com and http://map.norsecorp.com.

[336] See "DDoS attacks continue to rise in size, frequency and complexity. Are you prepared to stop them before they impact the availability of your business?" (Arbor Networks) <https://www.arbornetworks.com/ddos-protection-products>.

Most cyberattacks are conducted for financial reasons.[337] Conversely, DoS attacks are often carried out with political motives, as a demonstrative action against a particular website or online resource.[338]

II.V.I. DENIAL OF SERVICE ATTACKS AS POLITICAL CONTESTATION.

Digital forms of protest were first theorised in the mid 1990s. Their theoretical foundations are expressed in "Electronic Civil Disobedience and Other Unpopular Ideas", an essay published in 1996 by the new-media collective Critical Art Ensemble.[339] The work precisely analysed the sociological and technological changes that induced a "digital shift" in political protesting.

Digital techniques of contestation are a consequence of the social, political, and economic transformation happened during the digital era. Commercial, financial, and political streams gradually abandoned their traditional and tangible centres of power, in favour of digital sites.[340]

Traditional forms of protest are aimed at creating political pressure by hindering the normal functioning of key institutions. Due to the above-mentioned digital transformations, traditional protest has lost much of its effectiveness. Blocking the streets or the entrance to a public building can no longer obstruct political and economic forces, which are now largely digitalised.

In the 1990s, groups of politically motivated hackers started to perform acts of "electronic protest". They translated the traditional contestation tactics into cyberspace, by performing "net-strikes" or "virtual sit-ins". These protests consisted in the simultaneous digital presence of hundreds of online protesters (internet users), in the same digital space (a website), at a set time. The digital mass overwhelmed the resources of the target, temporarily blocking its functioning, and obstructing its availability to "legitimate" users, thereby denying them access to the service (i.e. Denial of Service attack).

---

[337] See e.g. J. Desjardins, 'Why Hackers Hack: Motives Behind Cyberattacks' (Visual Capitalist, 3 January 2018) <https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/>.

[338] See "DDoS Attacks 101: Types, targets, and motivations" (Calyptix, 26 April 2015) <http://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/>.

[339] Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Autonomedia & Critical Art Ensemble 1996).

[340] Let's consider, for instance, the commercial flux of a company. Today, it is not limited to the trucks entering or leaving its gates. Most of its external commercial activities are dealt with through the web.

At the dawn of the new millennium, the landscape of digital protest mutated slightly. Transnational collectives – such as the hacker collective "Anonymous" – were created. The number of attacks increased dramatically. Alongside DoS attacks, politically motivated hacker groups started to perform a wide range of cyberattacks, e.g. virtual sabotages, website defacements, website redirects, and information thefts.[341] Nonetheless, DoS attacks remain one of the most common cybercrimes and the one bearing the highest political significance, partially due to their analogical similarity to street rallies.

DoS attacks are cyberattacks aimed at exhausting the resources of a computer system in order to prevent its normal functioning and make it unavailable for its intended users. There are various types of DoS attacks.[342] Some target the application (e.g. through its HTTP[343]) or the network's resources. The majority of these attacks are "volumetric", meaning they consume the target's resources through a high volume of traffic (e.g. a large group of people refreshing a webpage, thus consuming its resources). Others, exploit a specific vulnerability of the targeted system.

The potential of a "volumetric" attack is amplified when it is contemporaneously launched from multiple computers. The amplification effect can be achieved in various ways. The earliest politically motivated DoS attacks were organised through "calls for action", directing protesters to connect to a given website at a given time. The whole mechanism was subsequently automatised. In 1998, the American media collective "Electronic Disturbance Theatre" developed the "Floodnet" software in order to simplify and automate participation in a virtual sit-in. The software, which is accessible online, automatically reloads the targeted web page every few seconds, thus reducing the effort needed from a virtual sit-in participant.[344] Several other tools were created with the purpose of automating attacks and coordinating protesters. Amongst them, Anonymous created and employed tools called "Low Orbit Ion Cannon" and "High Orbit Ion Cannon". These tools are equipped with a "Hivemind" feature, which transfers the control of the tool to a "master" user, who coordinates and directs the participants towards a determined target.

---

[341] See X. Li, 'Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime' (2013) 27 Harvard Journal of Law and Technology 301, 306 ff.

[342] See e.g. Radware Security, *DDoS Survival Handbook* (2015).

[343] The HyperText Transfer Protocol (HTTP) is the protocol used by the World Wide Web for formatting and trasmitting content.

[344] See B. Stalbaum, 'The Zapatista Tactical FloodNet: A collabortive, activist and conceptual art work of the net' (Tactical Media File, 07 August 2010) <http://www.tacticalmediafiles.net/articles/3394/The-Zapatista-Tactical-FloodNet> ("FloodNet is an example of conceptual net.art that empowers people through activist/artistic expression. By the selection of phrases for use in building the 'bad' urls, for example using 'human_rights' to form the url 'http://www.gb.mx/human_rights,' the FloodNet is able to upload messages to server error logs by intentionally asking for a non-existent url. This causes the server to return messages like 'human_rights not found on this server."); R. Dominguez, 'Electronic Civil Disobedience: Inventing the Future of Online Agitprop Theater' (2009) PMLA 1806, 1807.

Beside the voluntary participation of internet users, an attacker may use "botnets"[345], which are large collections of computers infected with a malware ("zombie" computers)[346]. These zombie machines are controlled by a "botmaster", who directs them to participate in the attack. Botnets were employed in the 2007 Estonian cyberattacks.[347]

There are many types of DoS attacks. Some exploit flaws and vulnerabilities in the target. Others use armies of infected computers to obstruct the correct functioning of a system. Importantly, some DoS attacks are generated by a voluntary massive presence of legitimate users in a digital place. On its own, each person is performing a licit online activity. Yet, the high number of requests cannot be handled by the system's resources, which thus become unusable. These forms of DoS attacks are the ones bearing the strongest resemblance to street protest. Accordingly, they are considered by many as legitimate acts of "electronic civil disobedience".

Several commentators have argued that DoS attacks should be subject to the same modes and limits set by the legal system with regard to physical street protest to balance criminalisation of political contestation and protection of fundamental rights (such as freedom of expression and assembly).[348] In 2013, a petition was posted on the White House's "We the People" website, claiming that DoS attacks must be considered a permissible form of protest.[349] However, while the sphere of criminal law came to embrace new criminal behaviours, and new legal interests translated in cyberspace, no

---

[345] A botnet is a network of internet-connected programs – called bots – which are under the control of the botnet's creator (the "bot herder" or "bot master"). The bots are usually spread through malware, with the aim of "recruiting" armies of unconsciously infected computers (so-called "zombie computers"), which are commanded and controlled by the botnet's operator.

[346] Botnets with millions of bots are not uncommon. The 'Conficker' worm, for example, has been estimated to have infected between 9 and 15 million machines.

[347] See G. Evron, 'Battling Botnets and Online Mobs Estonia's Defense Efforts during the Internet War' (2008) 9 Georgetown Journal of Intional Affaires 121. See *infra* § II.VI.III.

[348] See A. P Karanasiou, 'The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks' (2014) 28 International Review of Law, Computers & Technology 98; N. Scola, 'Ten Ways to Think About DDoS Attacks and "Legitimate Civil Disobedience"' (Techpresident, 13 December 2010) <http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacks-and-legitimate-civil-disobedience>; E. Morozov, 'In Defence of DDoS' (Slate, 13 December 2010) <http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html>; L. Oliva, 'Is DDoS the New 'Sit-In'?' (Vice, 25 January 2013) <http://motherboard.vice.com/blog/is-ddos-the-new-civil-disobedience>. For an analysis of a possible first amendment protection for politically-motivated cyber attacks, see X. Li, 'Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime'.

[349] See D. Kerr, 'Anonymous petitions U.S. to see DDoS attacks as legal protest' (CNet, 9 January 2013) <http://www.cnet.com/news/anonymous-petitions-u-s-to-see-ddos-attacks-as-legal-protest/>

"With the advance in internet technology, comes new grounds for protesting. Distributed denial-of-service (DDoS), is not any form of hacking in any way. It is the equivalent of repeatedly hitting the refresh button on a webpage. It is, in that way, no different than any 'occupy' protest. Instead of a group of people standing outside a building to occupy the area, they are having their computer occupy a website to slow (or deny) service of that particular website for a short time. As part of this petition, those who have been jailed for DDoS should be immediately released and have anything regarding a DDoS, that is on their 'records', cleared. [sic]"

extension of the right of assembly and protest has been made to cover such forms of political protest.

II.V.II. CRIMINAL REGULATION OF POLITICALLY MOTIVATED CYBERATTACKS.

Early criminalisation of DoS attacks.

The first "netstrikes" and "virtual sit-ins" hardly found a criminal repression, partially due to the lack of specific provisions criminalising DoS attacks. One of the first attempts to repress a virtual sit-in came in 2001, in relation to a digital protest against Lufthansa. An activist, whose role in the attack was mainly to register the website used to promote the attack, was prosecuted under section 240 of the German *Strafgesetzbuch* (offence of coercion). The first instance court of Frankfurt convicted him. However, the *Oberlandesgericht* (Higher Court) overruled the decision, holding that the virtual demonstration did not fulfil the criteria of "use of force" and "threat of appreciable harm" within the meaning of the offence.[350]

Over the period that followed, the growing incidence of DoS attacks,[351] together with society's increasing reliance on digital technology, amplified the need to protect the correct functioning and availability of computer systems. DoS attacks began to be subsumed under national cybercrime statutes. Most of these instruments, however, lacked specific consideration of DoS attacks. The majority of cyber specific criminal provisions were created in the 1990s to deal with other types of cybercrime, such as the creation and distribution of computer viruses or, more generally, illegal access to computer systems. Consequently, these instruments were unfit to cover the characteristics of DoS attacks. The necessary adaptation of the law was often left to judicial interpretation.

The UK system provides a perfect example of the problems encountered during the first criminalisation of DoS attacks. In the UK, the main legal instrument against cybercrime is the Computer Misuse Act 1990 (CMA). DoS attacks were subsumed under Section 3 of the Act, which covered "unauthorised modification" of computer material. As previously mentioned, some types of DoS attacks – and in particular "net-strikes" – exploit a licit process. They use legitimate traffic of a volume and a frequency sufficient to saturate the resources of the target.

---

350 GER, OLG Frankfurt 1, *Strafsenat 1 Ss 319/05, 22.05.2006.*

351 See e.g. Radware Security, *DDoS Survival Handbook* (n 342), 13.

The problem of whether these types of attacks were considered to be "unauthorised", in the sense employed in Section 3 CMA, was determined by case law. In a 2005 case of the Wimbledon Youth Court regarding an "email bombing",[352] the judge agreed with the defence that sending emails to an email server was a permitted behaviour and that "no reasonable tribunal could conclude that the modification caused by the emails sent by the defendant were unauthorised within the meaning of Section 3".[353]

On appeal, the High Court adopted a broader interpretation of the term and employed an argument of "implicit consent". The Court considered that, although the owner of a computer usually consents to the receipt of emails, such an implicit consent did not cover emails sent for the sole purpose of interrupting the operation of the system.[354] Following this argument, all internet traffic aimed at flooding the resources of a computer system, and impeding its correct functioning, was to be considered as "unauthorised".[355]

A further issue was related to the offence's requirement of an unauthorised "modification" of the contents of the computer system targeted (thus a permanent damage to the system).[356] Although early studies endorsed a broad interpretation of "modification", covering attacks that rendered data unreliable or impaired a computer's operation,[357] such a requirement was widely seen as a major hindrance to the adequate repression of DoS attacks.[358] In 2006, the CMA was amended following the UK's ratification of the CoE Convention on Cybercrime.[359] The 2006 Police and Justice Act removed the "modification requirement" from Section 3, broadening the *actus reus* from "unauthorised modification" to "unauthorised acts", and tailoring the offence to specifically address DoS attacks.

---

[352] An email bombing is a type of DoS attack. Huge numbers of emails are sent to an email server, which is overwhelmed by the load.

[353] UK, R v. Lennon, judgment of District Judge Kenneth Grant, sitting as a Youth Court in Wimbledon, 2 November 2005 (UK). See R. Clayton, *Complexities in Criminalising Denial of Service Attacks* (February 2006) <http://www.cl.cam.ac.uk/~rnc1/complexity.pdf>.

[354] UK, DPP v Lennon [2006] EWCH 1201.

[355] A similar problem is to be found in the US federal system (for the analysis of the authorisation requirement in the US Computer Fraud and Abuse Act see J. McLaurin, 'Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks' (2011) Yale Law & Policy Review 211, 228).

[356] See L. Edwards, 'Dawn of the death of distributed denial of service: How to kill zombies' (2006) 24 Cardozo Arts & Entratainment Law Journal 23, 36 ff.

[357] See Internet Crime Forum Legal Subgroup, *Reform of the Computer Misuse Act 1990* (April 2003) <http://www.internetcrimeforum.org.uk/cma-icf.pdf>.

[358] See R. Clayton, *Complexities in Criminalising Denial of Service Attacks* (n 353).

[359] See S. Fafinski, 'Computer misuse: The implications of the Police and Justice Act 2006' (2008) 72 The Journal of Criminal Law 1, 53.

The Budapest Convention on Cybercrime.

The necessary adjustments for national provisions aimed at repressing DoS attacks were eventually provided by the international instruments on cybercrime.

In the Council of Europe Convention on Cybercrime, DoS attacks are covered by Article 5 on system interference, which is aimed at providing a minimum level of protection to the legal "interest of operators and users of computer or telecommunication systems [in] being able to have them function properly".[360] This provision sets a qualitative threshold before activation of liability, namely the "serious" hindering of the functioning of a computer system. This threshold have a critical importance with regard to DoS attacks.

As previously pointed out, according to the Explanatory Report to the Convention, "serious" hindering means the "sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems".[361] The text of the Convention does not precisely outline the concept of seriousness, leaving each State party free to define it. However, in order to avoid overcriminalisation, the Convention suggests that member States determine the sanction in relation to the extent to which the functioning of the system is hindered (partially or totally, temporarily or permanently).[362] Theoretically, this suggestion may exclude from the scope of the offence particular types of DoS attacks, possibly providing a space for licit digital "blockades".

However, as noted in the CoE study on the national implementation of the Budapest Convention, national provisions "could be broader than the Cybercrime Convention, covering all attempts to interfere, and not just the serious hindering".[363] Many systems lack a gravity threshold for liability to arise. For example, the French system carries a sentence of imprisonment up to five years or a fine, for anyone convicted of interfering with the functioning of a computer system, regardless of the gravity of the interference.[364]

Even those systems that determine criminalisation based on the amount of harm produced by an act may not leave space for licit political protests performed through DoS attacks. The degree of damage produced by a DoS attack is modelled as similar to that produced by a street rally.[365]

---

[360] CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 65.

[361] *Id.* § 67 (emphasis added).

[362] *Id.* at § 69.

[363] L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 23.

[364] FR, *Code Pénal*, Article 323-2.

[365] Obviously, if the target service is not essential.

Financial losses are mostly indirect and can include loss of business (e.g. customers are unable to access a website), cost of IT security, and loss of reputation. The sole direct damage is related to countering the attack and restoring the service.

In the US federal system, DoS attacks fall under the scope of the 18 US Code § 1030(a)(5)(A), which punishes actors who "knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer". At its basic level, the offence provided for in 18 USC § 1030 (a)(5)(A) is a misdemeanour. If the attack causes sufficient loss or other specified harm,[366] the penalty increases in severity and the crime is considered a felony.[367] The term "loss", however, includes indirect damage to the computer system. It encompasses "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service".[368] The harm threshold provided by the norm is thus easily surpassed by any type of DoS attack. In 2013, following series of DoS attacks conducted by Anonymous members (so called "Operation Payback"), a federal grand jury in Virginia indicted 13 hackers under the 18 USC § 1030(a)(5)(A).[369] According to the indictment, the attacks produced "at least $5000" of damage (the specifics of which, however, remain unclear). [370]

The Budapest Convention itself is less than clear on this issue. However, Article 5 was not interpreted as leaving room for licit acts of cyber protest. The CoE study on the national implementation of the CoE Convention even proposed bypassing the damage criterion, deeming it

---

366 US, *United States Code*, Title 18, § 1030 (c)(4)(A)(i): (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (VI) damage affecting 10 or more protected computers during any 1-year period.

This subsection was introduced by the *2001 Patriot Act*, and codifies the decision of *US v Middleton*, 231 F 3d 1207 (9th Cir 2000). The US Patriot Act also amended the definition of "damages", which now covers "any impairment to the integrity or availability of data, a program, a system, or information". Such a broader definition is likely to cover the temporary obstruction of the functioning of a computer system (see: H. Marshall Jarrett and M. W. Bailie, 'Prosecuting Computer Crimes' (2010) Office of Legal Education - Executive Office for United States Attorneys, 39). In this direction went the US Sixth Circuit Court of Appeal, which stated that "a transmission that weakens a sound computer system – or, similarly, one that diminishes a Plaintiff's ability to use data or a system – causes damage" in the meaning of 18 USC § 1030 (a)(5)(A) (US, *Pulte Homes, Inc. v Laborers' Intern Union of North America*, 648 F 3d 295 [6th Cir 2011]).

367 18 USC § 1030 (c)(4)(B)(i).

368 US, *United States Code,* Title 18, § 1030 (e)(11).

369 US, *United States v. Dennis Collins, et.al.*, No. CR 11-00471 DL.

370 US, *United States v. Dennis Collins, et.al.*, 1:13-cr-383 (2013), §3.

advisable that the Convention "should also criminalize the new cyber threats such as Net-strike, DoS, DDoS, or Mail-bombing attacks, that do not necessarily cause in each case a damage in the form of a serious hindering, but only a menace for the functioning of the system as the (partially or fully) obstacle or interruption of the functioning of the system".[371] Eventually, a 2013 Guidance Note to the Convention recognised the full coverage of DoS attacks by Article 5, stating that the objective of a DoS attack "is precisely to seriously hinder the functioning of a computer system"[372]. Moreover, it suggested amendments to domestic law where sanctions were "unsuitably lenient".[373]

The minimum criminalisation standard set by the CoE Convention in order to protect the proper functioning of computer systems is currently interpreted as completely covering DoS attacks, irrespective of the type of attack, the motivation, or the damage produced.

The EU Framework.

In the European Union, Article 3 of the 2005 Framework Decision and Article 4 of the 2013 Directive on attacks against information systems criminalise not only the DoS attacks which cause serious hinderance, but also any interruption of the functioning of an information system more generally. These instruments do however leave open the option to criminalise such conduct only "for cases which are not minor". The Commission's Report on the implementation of the Framework Decision[374] noted that six member States used this option. It considered that a more refined definition of "cases which are not minor" was required, and suggested that this concept could refer to cases where "the system interference as such is of minor importance or where the integrity of the information system is only interfered with to a minor degree".[375]

Due to the growing reliance of State's critical infrastructures on digital technology, the correct functioning of computer systems is increasingly interlinked with other essential interests (e.g. public

---

371 L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 24.

372 CoE, Cybercrime Convention Committee, *Guidance Note #5 DDOS Attacks*, T-CY (2013)10E Rev, 5 June 2013, 4.

373 *Ibidem.*

374 EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148).

375 CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 5.

health or national security). As a result, the political significance of cyberspace has augmented. The number of politically motivated cyberattacks confirms this interpretation.[376]

In consideration of scenarios such as large-scale cyberattacks against critical infrastructures, concerns over the threat posed by cyberattacks has grown, demanding their stringent criminalisation. As pointed out in the preamble to the EU Directive, "attacks against information systems, and, in particular, attacks linked to organised crime, are a growing menace in the Union and globally, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and of the Union". The international framework increased the penalties provided for the offence of system interference and specifically addressed the operational traits of politically motivated DoS attacks.

Aggravating circumstances were already provided by Article 7 of the EU 2005 Framework Decision. On the basis of that provision, the offence of system interference was to be punished with a maximum term of imprisonment of between two and five years when committed within the framework of a criminal organisation (as defined in Joint Action 98/733/JHA), causing serious damages, or affecting essential interests.

Following the implementation of this provision, the German *Strafgesetzbuch* was amended to impose a penalty of imprisonment of between six months and ten years for serious cases of "computer sabotage". According to §303b *Strafgesetzbuch*, a serious case "usually occurs" when the crime causes major financial loss, or the offender acts on a commercial basis or as a member of a criminal consortium whose purpose is the continued commission of computer sabotage, or the offence jeopardises the population's supply of vital goods and services or the national security of the Federal Republic of Germany.[377]

---

[376] EU, *Summary Of The Impact Assessment Accompanying Document to the Proposal for a Directive of the European Parliament and of the Council on Attacks Against Information Systems, and Repealing Council Framework Decision 2005/222/JHA,* [2010] SEC(2010) 1123 Final, 2; EU, *Accompanying Document to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience' – Summary of the Impact Assessment,* [2009] COM(2009) 149 SEC(2009) 399, 3.

[377] GER, *Strafgesetzbuch*, § 303b.

In the 2013 EU Directive, the penalties were raised to a maximum term of imprisonment of at least five years, and the aggravating circumstance of attacks affecting an essential interest was replaced by one of attacks committed against critical infrastructures.[378]

In 2013, the Guidance Note to the CoE Convention on DoS attacks recommended that the Parties consider "damage to critical infrastructures" to be an aggravating circumstance. As pointed out by the US Seventh Circuit Court of Appeals: "the penalty for crippling an emergency-communication system on which lives may depend should be higher than the penalty for hacking into a Web site to leave a rude message."[379]

Politically motivated DoS attacks as licit digital protest?

DoS attacks were theorised in the 1990s as a new method of political protest. In an era of digital economy and politics, virtual sit-ins were conceived as a necessary tool for political contestation.

A DoS attack blocks a digital place – a virtual container of political or financial power – and its methods and effects are readily comparable to a physical sit in. Although this analogy was strongly defended by digital protesters, no extension of the balancing between criminal repression and the right to (digital) expression, assembly, and protest was provided by domestic or international cyber legislation. The criminal law of most States represses illegal interference with computer systems without providing distinctions between the various forms of DoS attacks. In a bid to reinforce the protection of computer systems, politically motivated DoS attacks are now sanctioned with very high penalties, including periods of imprisonment ranging from 5 to 10 years.

So far, no legal system explicitly recognises a right to digital protest through DoS attacks. As most international and domestic provisions on the right to association and assembly were formulated prior to the "digital revolution", no direct reference to digital forms of protest can be found therein.

From a general point of view, two UN General Assembly Resolutions (68/167 of 18 December 2013 and 69/166 of 18 December 2014) recognised the need for equal protection between online and offline expressions of fundamental human rights. In 2012, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association called upon States "to recognize that the rights to freedom of peaceful assembly and of association can be exercised through new

---

[378] EU, *2013 Directive on attacks against information systems* (n 83), Article 9 (4)(c). A further step towards the criminalisation of DoS attacks has been taken by the 2013 EU Directive. It expressly envisaged the criminalisation of the intentional production, sale, procurement for use, import, distribution or otherwise making available of a computer program, designed or adapted primarily for the purpose of committing any of the offences referred in the Directive – thus covering botnets and other tools such as those automating the attack and coordinating protesters.

[379] US, *United States v. Mitra*, 04/18/2005, 04-2328 - US 7th Circuit.

technologies, including through the Internet".[380] However, such statements are likely to be related to the use of the Internet as a tool for organising and managing physical assemblies.[381] The only (non-binding) international instrument specifically taking digital protests into account is the CoE Recommendation CM/Rec(2014)6 "Guide to human rights for Internet users".[382] The recommendation states that everyone has: "the right to peacefully assemble and associate with others using the Internet. In practice, this means: 1. you have the freedom to choose any website, application or other service in order to form, join, mobilise and participate in social groups and assemblies whether or not they are formally recognised by public authorities. You should also be able to use the Internet to exercise your right to form and join trade unions; 2. you have the right to protest peacefully online. However, you should be aware that, if your online protest leads to blockages, the disruption of services and/or damage to the property of others, you may face legal consequences".[383]

In this Recommendation, criminal law limitations to digital protest are explicitly recognised. Interestingly, the qualitative threshold envisaged in the recommendation appears similar to the CoE Cybercrime Convention's threshold of "serious hindering" (blockages, disruption, damage), possibly excluding those politically motivated DoS attacks causing only minor or temporary hindering.

In the CoE system, no case law has approached the issue of digital protest in light of Article 10 (freedom of expression) or Article 11 (freedom of assembly and association). The 2014 CoE Report on freedom of assembly and association on the Internet explicitly deals with the right to protest online, defining it a "controversial issue".[384] The Report appears open to partially recognising a right to electronic civil disobedience through DoS attacks. On the one hand, it acknowledges that: "interferences with computer functioning can fall under the scope of the Convention on Cybercrime of the Council of Europe"; "such interferences can constitute criminal actions and many of them may in fact have very negative effects on the rights to freedom of expression, peaceful assembly, association or the right to property"; and "the persons who decide to engage in act of civil

---

[380] UN GA, Human Rights Council, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai*, A/HRC/20/27, 21 May 2012, at A.84(k).

[381] See generally, CoE, *Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet*, MSI-INT (2014)08 rev6 Final, 10 December 2015.

[382] CoE, *Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users*, CM/Rec (2014)6, 16 April 2014.

[383] *Id.*, 4.

[384] CoE, *Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet* (n 381).

disobedience may be punished by the law"[385] (although it stresses that, in such a case, particular attention should be paid to the proportionality of the sanction).[386]

However, on the other hand, the Report supports the argument that digital protests are covered by freedom of expression and peaceful assembly, recalling that "(a)n assembly should be deemed peaceful if its organizers have professed peaceful intentions and the conduct of the assembly is non-violent. The term "peaceful" should be interpreted to include conduct that may annoy or give offence, and even conduct that temporarily hinders, impedes or obstructs the activities of third parties."[387]

Most importantly, it recognises the limits of the existing international cybercrime framework, advocating an analytical framework "which would be able to address specific elements such as intent (to protest or express political or social dissent, to get the attention of the general public and contribute to the political debate) and overall impact (causing of temporary harm as opposed to permanent negative consequences for the general public), and to put in balance all these considerations."[388]

Therefore, the Report suggests that States differentiate between online (licit) protest and malicious (illicit) attacks at the normative level by specifying the norm with two qualifying constitutive elements. As pointed out *supra*, such differentiation is lacking in the existing national and international cybercrime framework.

As well as dealing with the above-mentioned issues, any normative solution aimed at considering the right to digital protest must address a series of additional problems.

The first of these problems relates to the balance between the property rights of the people affected by such a protest, and the right of protesters to peaceful assembly. On this point, the Office for Democratic Institutions and Human Rights of the Organisation for Security and Cooperation in Europe Guidelines on Freedom of Peaceful Assembly stated: "The regulatory authority has a duty to strike a proper balance between the important freedom of peaceful assembly and the competing rights of those who live, work, shop, trade, and carry on business in the locality affected by an assembly (...) Given the need for tolerance in a democratic society, a high threshold will need to be

---

385 *Id.*, 18.

386 *Id.*, 19.

387 *Id.,* 17-18. CoE, Venice Commission, Office for Democratic Institutions and Human Rights of the Organisation for Security and Cooperation in Europe, J*oint Guidelines on Freedom of Peaceful Assembly of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights*, 2010, 15. See also, *inter alia*, ECtHR, *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria*, (Application n. 29221/95 and 29225/95) 2 October 2001.

388 CoE, *Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet* (n 381).

overcome before it can be established that a public assembly will unreasonably infringe the rights and freedoms of others".[389]

Differences between physical and digital protests should be acknowledged. The right to assembly is usually protected in public places, where the above mentioned balance tends towards the right to protest (although every protest has indirect repercussions for private properties neighbouring the public space where the protest is held).[390] Conversely, such a right is afforded with lesser or no protection in relation to privately owned places, where protest is conducted against the will of the owner of the space.[391] In such cases, the balance between property and assembly rights is weighted in favour of the former.

In terms of online protest, the pivotal problem is that, today, there are no online public spaces. Every digital place is privately owned, even though the "quasi-public"[392] nature of the Internet has been highlighted by many scholars and human rights activists, hinging on its primary communicational and social functions.[393] Moreover, the existing cybercrime framework is strongly inclined to protect the property rights of the owner of the computer systems targeted by the attack.

However, in a case about a protest in a privately-owned shopping centre, the European Court of Human Rights recognised that the right to freedom of association may involve access to private property, where such access is the only effective way of exercising the right.[394] This appears to be so in the case of the Internet, where – due to the network's structure – protesting necessarily requires access to private property. In a digital world where all roads and squares are owned by corporations, it cannot be expected that one completely renounces his/her right to assembly and protest.

---

[389] CoE, Venice Commission, Office for Democratic Institutions and Human Rights of the Organisation for Security and Cooperation in Europe, J*oint Guidelines on Freedom of Peaceful Assembly* (n 387). See also ECtHR, *Ashughyan v. Armenia* (*Application n. 33268/03*), 17 July 2008, § 90. Similarly, see ECtHR, *Balçık and Others v. Turkey* (*Application n. 25/02),* 29 November 2007, § 49; ECtHR, *Oya Ataman v. Turkey* (Application n. 74552/01) 5 December 2006, § 38.

[390] See e.g. ECtHR, *Aldemir v Turkey* (Application n. 32124/02), 18 December 2007, § 43: "Any demonstration in a public place may cause a certain level of disruption to ordinary life and encounter hostility."

[391] See J. Slobbe and S. L. C. Verberkt, "Hacktivists: Cyberterrorists or Online Activists?" (2012) arXiv preprint arXiv:1208.4568, 7; X. Li, 'Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime' (n 341), 313ff.

[392] See, on the protection of freedom of expression in "quasi-public" *fora* in the US system, A. Maniscalco, 'Public Spaces, Marketplaces, and the Constitution: Shopping Malls and the First Amendment' (SUNY Press, 2015); US, *Shad Alliance v. Smith Haven Mall,* 66 NY2d 496, 502 (1985).

[393] With particular reference to the Internet, see Article 19, *The "Right to Protest": Background paper* < https://right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf>, 23; W. Benedek and M. C. Kettemann, *Freedom of expression and the Internet* (Council of Europe, 2014), 102ff;

[394] ECtHR, *Appleby and Others v. The United Kingdom*, (Application No. 44306/98), 6 May 2003, § 47, "Where, however, the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights. A corporate town where the entire municipality is controlled by a private body might be an example."

A final problem relates to the ease with which DoS attacks can be organised and carried out. In comparison with a street rally, digital protests require less organisational and financial efforts. DoS attacks can be conducted more frequently than physical protests, constituting a major nuisance to the functioning of the Internet. With reference to this, it makes sense to differentiate between virtual sit-ins with a one-to-one ratio (one protester, one request) and DoS attacks conducted with the use of infected computers (botnets), which unconsciously participate in the attack. The latter type of protest clearly breaks with the analogy with physical street protests. Such acts more closely resemble hijackings than acts of protest. For the sake of recognising a licit space of virtual protest, such technically-enhanced cyberattacks (using botnets) should be firmly distinguished from those conducted, with political motivations, by a mass of online protesters.

Any ideal normative framework recognising DoS attacks as a licit form of protest should, first and foremost, be expressed via a reform of cybercrime law. A more precise material element of damage may exclude from the scope of the offence of system interference digital protests causing a temporary hindering of the functioning of a system. Furthermore, a more precise mental element of specific intent may exclude acts conducted with the aim of expressing political dissent.

Further conclusions can be drawn from a parallelism between digital and physical protest. The method of the attack could be taken into consideration, criminalising the use of botnets. Moreover, providing appropriate mechanisms for online protesters to be formally authorised by a competent body[395], could prevent the risk of (digital) violence and excessive harm to the rights and freedoms affected by an online protest.[396] Finally, more lenient sanctions could be provided for unauthorised digital protest: with regards to physical protests, illicit acts are normally treated as infractions or misdemeanours.[397] This principle could be extended to digital protest.

---

[395] Considering that such a "competent authority" currently does not exist, could it be an international body, due to the jurisdictional problems related to endorsing a national body (e.g. country from where the attack is organized, or the one of the ITC attacked) with such power?

[396] See, e.g., ECtHR, *Rassemblement Jurassien and Unité Jurassienne v Switzerland* (Application n. 8191/78) 10 October 1979; CoE, Venice Commission, Office for Democratic Institutions and Human Rights of the Organisation for Security and Cooperation in Europe, *Joint Guidelines on Freedom of Peaceful Assembly* (n 387), 17.

[397] See M. Sauter, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet* (Bloomsbury, 2014), 142.

II.VI. CYBERATTACKS AS TERRORISM.

As previously noted, with particular regard to attacks against critical infrastructures, cybercrime may acquire a transnational and – to a certain extent – supranational dimension. This phenomenon has been here called the "quantitative" extension of the underlying legal interests. This "spatial" extension of cybercrime may influence the jurisdictional issues underlying its repression. In the case of malicious cyberactivity harming or endangering an international interest, the fora of regulation and enforcement may show a tendency to internationalisation. Undoubtedly, this tendency is *in fieri:* no substantive offence is directly applicable at the international level. Nor is there an international tribunal with jurisdiction on cybercrime.

A further issue is that of the "qualitative" extension of the underlying legal interests, i.e. the modification of the values contained in computer systems and digital data due to socio-technological evolution. The more cyberspace is used and filled with data that have to be protected against attacks, the more the norms constructed to regulate cybercrime are imbued with content. This reveals that the problem of categorisation is one of the crucial issues with regard to the legal approach to the cyber world. As described *infra*, this issue is partially related to the inability of the legislator to completely grasp digital phenomena, and is mainly linked to the fast-changing nature of the technological world. Similar to quantum mechanics, in order to describe how a legal particle can be located in different positions at the same time, the law may depict the targeted digital behaviour according to all forms and positions it can assume. However, while the observed particle is resting inside the normative box, it is also changing. The result of this is that, like Schrödinger's cat, when we observe the content of the box, we find that the cat is neither dead nor alive, but following technological reform has changed into something different. Furthermore, we may also discover that other animals have entered the box. The solution is either to change the box as frequently as possible, or to construct bigger boxes. The latter seems to be the solution adopted most frequently. Both strategies, however, admit different drawbacks.

Cybercrime offences may cover a wide series of behaviours, from the breach of contract of an online service to attacks against critical infrastructures. This subchapter will evaluate how the existing legal framework addresses the most serious cyberattacks. In particular, it will consider what happens when these attacks can be labelled as terrorism. The result of the analysis, interestingly, shows that occasionally creating a wrong "box" can be less effective than relying on the already-existing ones.

II.VI.III. CYBER TERRORISM IN THE INTERNATIONAL INSTRUMENTS.

The exponential growth of international terrorism fuelled the demand for an international framework covering terroristic offences.[398] In Europe, the high degree of legal and political homogeneity has enabled a strong unitary reaction to international terrorism, with the enactment of important treaties on the topic: the 1977 European Convention on the Suppression of Terrorism[399] adopted under the aegis of the Council of Europe, and three instruments adopted by the EU with the aim to harmonise the various national systems towards a common definition of terrorism.[400] As a matter of fact, in 2001 only six out of fifteen E.U. Member States have had a specific offence for terrorist acts in their criminal law. These were largely the countries that previously faced significant internal terrorism.[401]

---

[398] According to Bobbitt (See: P. Bobbit, *Terror and Consent* (Alfred A. Knopp 2008), 24), terrorism exists as an "epiphenomenon of the constitutional order". It mutates as the constitutional order mutates, changing, together with the constitutional order, in its form and its targets. State nations generated anarchist terrorism, whose targets where the high officials representing the State, while industrial nation-state brought revolutionary terrorism, which was attacking local representatives of the material well-being of the people, on which the State was confirming its legitimacy. In the age of the "market state", terrorism is "just as global, networked, decentralized and devolved" as the state. In other words, in a globalized world, terrorism has become globalized. Is the "digital age" creating a new type of terrorism?

[399] CoE, *European Convention on the Suppression of Terrorism*, ETS No. 90, 27 January 1977.

[400] EU, *Joint action of 21 December 1998 98/733/JHA adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union*, OJ L 351, 29.12.1998, EU, *Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism,* OJ L 164, 22.6.2002, EU, *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, OJ L 330, 9.12.2008.

[401] Namely: France, Germany, Italy, Portugal, Spain and United Kingdom.

At the international level, however, any attempt at a comprehensive definition of international terrorism has failed. The efforts toward enacting a common, comprehensive convention on terrorism have suffered due to the political divergences between States. States have largely been unable to reach a consensus on specific sensitive issues (especially on acts of terrorism carried out during wars of liberation, or by the so called "freedom fighters", and covered by the principle of the self-determination of peoples).

While their scope is far from being at a level of a general application, general definitions of terrorism are to be found in UN resolutions and, in particular, in the 1999 Convention for the Suppression of the Financing of Terrorism.[402]

As a result of this international stalemate, a plethora of international conventions and protocols on terrorism have been adopted. These instruments combat terrorism through a specific, or sectorial, approach. They define and proscribe specific types of terrorist conducts, such as taking of hostages and hijacking. Most were implemented in reaction to topical terrorist incidents.[403]

---

[402] See also Special Tribunal for Lebanon, Appeal Chamber, *Interlocutory Decision on the Applicable law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, Case No. STL-ll-0111, 16 February 2011. According to the Appeal Chamber, "a number of treaties, UN resolutions and the legislative and judicial practice of States evince the formation of a general opinio iuris in the international community, accompanied by a practice consistent with such opinio, to the effect that a customary rule of international law regarding the international crime of terrorism, at least in time of peace, has indeed emerged". The elements of the customary rule are, according to the Court: "the perpetration of a criminal act, or threatening such a act (such as murder, kidnapping, hostage-taking, arson, and so on); the intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it; the act must have a transnational element".

[403] See B. Saul, Defining Terrorism in International Law, 180 (OUP 2008).

In 2007, Estonia was struck by a series of politically motivated DoS attacks. The attacks "brought down important parts of the critical information infrastructure in government and the private sector for days."[404] The massive cyberattack was implemented by organised and politically motivated hacker groups, in all likelihood supported by Russia, and targeted essential State interests. Naturally, the event stimulated a wide debate on whether such attacks could (or should) be framed as terrorism, or even as acts of war[405].[406]

However, most of the concern around the terroristic use of digital technology has been embodied in the framework criminalising common cyber offences. No international treaty on cyberterrorism has so far been adopted at the regional or international levels.

Notwithstanding the constant rise in the scale of attacks and their increasing transnational character – as clearly exemplified by the Estonian case, or by the 2015 and 2016 attacks on the Ukrainian power grid – [407] no clarification on the qualification of cyber acts of large-scale or transnational character is to be found in the existing cybercrime framework.

---

[404] EU, *Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA,* [2010] COM(2010) 517 Final, OJ C 218, 23.7.2011, § 2.7.

[405] At least in political and media discourse, there is a tendency to categorise certain types of cyberattacks as cyberterrorism or cyber war. Performing the search <Estonia + "cyber war"> on Google Scholar and Google Web, we find about 4.010 and 73.300 results respectively. On the search <Estonia + cyberterrorism>, about 1,650 and 44,600 results (search performed the 10th of January 2020). Such disposition, however, is also detectable in more official environments. A leaked document from the New York State Division of Criminal Justice Services, for instance, reports that one of the prominent members of Anonymous was categorised as a "possible terrorist organisation member". Document retrievable at <https://www.documentcloud.org/documents/1532943-jeremy-hammond-dcjs-document.html>.

[406] In the aftermath of the attack, Estonia's foreign minister stated that "at present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country. Not a single Nato defence minister would define a cyberattack as a clear military action at present. However, this matter needs to be resolved in the near future." (See I. Traynor, 'Russia accused of unleashing cyberwar to disable Estonia' (The Guardian, 17 May 2007) <http://www.theguardian.com/world/2007/may/17/topstories3.russia>). Undoubtedly, hacker groups have extended their activities into armed conflicts involving States. During the 2008 South Ossetia military campaign, patriotic hacker collectives (very possibly under the direction of the Russian government) conducted intensive cyberattacks against Georgian digital systems. In 2012, as a response to the Israeli military operation in Gaza 'Pillar of Defence', Anonymous launched DoS attacks against several Israeli websites and posted online names, ID numbers and personal emails of 5,000 Israeli Defence Force officials. In 2014, the hacker collective launched two operations (OpRussia and OpUkraine) striking Russian cyberspace in reaction to the Russian maneuvers in Crimea. On the role of non-state actors in cyber warfare and their impact on ius in bello and ad bellum see N. Bussolati, 'The Rise of Non-State Actors in Cyberwarfare', in C. Finkelstein, J. David Ohlin and K. Govern (Eds), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015). However, the issue of whether a cyberattack can be considered to be a use of force within the meaning of Article 2(4) of the UN Charter is beyond the scope of this work.

[407] See "Ukraine power cut 'was cyber-attack'" (BBC, 11 January 2017) <http://www.bbc.com/news/technology-38573074>.

In the absence of an international treaty, some States have autonomously regulated the phenomenon of cyberterrorism, largely by providing terrorist offences with additional material elements covering cyber acts. Conversely, where no cyber-specific terrorism offences have been enacted, the State is left to rely either on existing terrorist offences, or on the common cybercrime framework.

II.VI.IV. CYBERTERRORISM AS A NEW BREED OF TERRORISM.

The majority of western legal systems have faced two types of terrorism: internal politically motivated terrorism[408] and international, religiously or otherwise ideologically motivated terrorism. Hence, modification in the main traits of terrorism, and related legal reforms, have largely revolved around the motivation for the act, and its transnational character.

The fundamental legal question connected to cyberterrorism is whether States need a new regulation to deal with cyberterrorism, or whether, *per contra*, such phenomenon could be adequately addressed by the existing terrorism and cybercrime frameworks. Any answer should consider the extent to which cyberterrorism represents a new breed of terrorism.

Contemporary terrorism includes various specific criminological morphologies: e.g. bioterrorism, chemical terrorism, radiological terrorism, etc. All definitions of the different species of terrorism are composed of the word terrorism, and a prefix indicating – more than the area of application – the "tools" employed in the commission of crime. For example, chemical terrorism is a serious criminal act committed with the special terrorist intent via the use of chemical agents. The fixed elements, which define the genus, are the special intent and the seriousness of the act.

As pointed out by Barry Collin – one of the first scholars to address the issue of cyberterrorism – crimes of this sort contain peculiar traits, which transcend the mere employment of digital tools. Indeed, more than in the case of ordinary cybercrime, cyberterrorism is the product of the convergence of two realms: the digital and the physical.[409] The legal appreciation of cyberterrorism mainly depends on the extent of this convergence, which is hypostatised in the material element and in the intended result of the crime.

---

[408] See, e.g., M. Clementi, Storia delle Brigate Rosse (Odradek, 2007); I. Sànchez-Cuenca, "The Dynamics Of Nationalist Terrorism: ETA and the IRA", (2007) 19 Terrorism and Political Violence 289.

[409] See B. Collin, "The Future of Cyberterrorism: The Physical and Virtual Worlds Converge", (1997) 13 Crime & Justice International Journal 15.

II.VI.V. THE USE OF ORDINARY TERRORIST OFFENCES.

Where no reforms aimed at providing the legal system with specific cyberterrorism offences have been carried out, the State is left with no options other than to rely on ordinary cybercrime provisions[410] or on traditional terrorism offences. A cyber act is labelled as terrorism when, rather obviously, it fulfils the constitutive elements of a terrorist offence. Hence, the coverage of cyberattacks depends on an analogical comparison with non-cyber activities falling under the scope of the terrorist offences.

In most definitions, the mental element is composed of a two-folded special intent to spread fear among the population, or else to directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it.[411] Furthermore, antiterrorism legislation usually addresses acts causing serious harm to persons and property. The conduct must therefore have a qualitative threshold of seriousness. The two elements – mental and material – are inherently correlated, since fear and coercion can be generated only by particularly serious criminal acts.

When considering cyberterrorism, the material element of the crime is of particular importance, whereas the mental element (being placed in the mind of the perpetrator) is separated from the digital realm. The above-mentioned analogical comparison between the digital and physical realms is mainly based on the material element of the crime and, more specifically, on criteria around the scale and effect of the act. A cyberattack constitutes an act of terrorism when the perpetrator possesses specific terrorist intent and the act is intended to produce a harmful physical event of sufficient gravity to fall within the scope of antiterrorism provisions.

Let's use as an example the definition of terrorism laid down in the 1999 International Convention for the Suppression of the Financing of Terrorism[412]. After referring to acts specifically prohibited by various international conventions, the convention provides – in Article 2.1 – a definition of terrorism. To this purpose, it refers to: "any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act".

---

[410] In case of a terrorist use of the web not meeting the qualitative threshold of the terrorist offences, the State may apply ordinary cyber offences. The increased gravity of the act will likely be considered at the sentencing stage, relying on the range of punishment provided by the ordinary cyber norm. Yet, considering that such range has diachronically undergone a substantial rise, specifically in order to take into account particularly serious cyberattacks, the provided punishment will be able to wholly cover the degree of harm expressed by the act.

[411] See, *inter alia*, UN, *International Convention for the Suppression of the Financing of Terrorism*, Treaty Series vol. 2178, p. 197; Adopted by the General Assembly Resolution A/RES/54/109, 9 December 1999.

[412] *Id.*

However, aside from extreme cases (e.g. shutting down the digital power grid control of a hospital, and, as a consequence, its life support equipment), such a degree of harm is unlikely to result from a cyberattack.

However, being a crime that substantially harms or endangers the public interest of national security, most terrorist offences are not exclusively limited to acts causing serious harm to persons, and may involve damage to public property, in particular to critical infrastructure.

For instance, Article 2 of the Draft Comprehensive Convention on International Terrorism[413] defines terrorism as: "an act intended to cause: death or serious bodily injury to any person; or serious damage to a State or government facility, a public transportation system, communication system or infrastructure facility with the intent to cause extensive destruction of such a place, facility or system, or where such destruction results or is likely to result in major economic loss; when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act"[414].

This type of terrorist offence could cover cyberattacks directed towards digitalised critical infrastructures that meet the qualitative threshold of seriousness (i.e. the intent to cause serious damage, extensive destruction, or major economic loss). A cyberattack targeting digitalised essential public systems (e.g. power utilities, transportation systems, or communications networks) such as the 2015 and 2016 attacks against Ukrainian infrastructures, which left thousands without electricity,[415] may fulfil the norm without the need for a "chain reaction" creating, from data interference, subsequent physical effects.

---

[413] In 1996 the General Assembly, with Resolution 51/210 of 17 December (UN GA Resolution A/RES/51/210, 17 December 1996), decided to establish an Ad Hoc Committee with the assignment of – *inter alia* – develop a comprehensive legal framework of conventions dealing with international terrorism. To this Committee, and to the Working Group of the General Assembly's Sixth Committee, was given the task to begin consideration with a view to the elaboration of a Comprehensive Convention on International Terrorism (see UN GA, Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996, Sixth session (28 January-1 February 2002, A/57/37).

[414] *Id.*, Art. 2.

[415] See "Cyber Attacks on the Ukrainian Grid:

What You Should Know" (FireEye, 2016) <https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf>; J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks" (MIT Technology review, 22 December 2016), <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/>.

II.VI.VI. THE ENACTMENT OF SPECIFIC CYBER TERRORISM OFFENCES.

In the absence of an international definition of cyberterrorism, some national systems have autonomously enacted specific cyberterrorism offences.[416]

In the aftermath of the aforementioned 2007 cyberattacks, Estonia reformed its antiterrorist framework. Article 237 of the Estonian Criminal Code now provides for an offence of terrorism with a material element that includes the "interference with computer data or hindrance of the operation of computer systems".[417] The offence – punishable by 5 to 20 years' imprisonment or life imprisonment – requires the typical specific *mens rea* of an intent to "force the State or an international organization to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the State, or to seriously interfere with or destroy the operation of an international organization, or to seriously terrorize the population". The European Economic and Social Committee recognised the enactment of this offence as good practice providing a "strong message to criminals and to citizens seeking reassurance".[418] Undoubtedly, the move gave greater clarity to a previously grey area in the regulation of cyberattacks, serving the principle of legality.

A similar normative construction can also be found in the UK system.[419] The UK Terrorism Act 2000 criminalises, *inter alia*, acts "designed seriously to interfere with or seriously to disrupt an electronic system".[420] To fall under the scope of this provision, an act must be "designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public" or "made for the purpose of advancing a political, religious, racial or ideological cause".[421] Here, both the *actus reus* and the *mens rea* are broader than those of the equivalent Estonian provision. Although a degree of seriousness is envisaged, a cyber act does not have to concretely generate an interference or disruption. It is sufficient for an act to be "designed"

---

[416] On the analysis of the legal definitions of cyber terrorism and related offences in United Kingdom, Australia, Canada and New Zealand see K. Hardy and G. Williams, 'What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism' in T. Chen, L. Jarvis, S. Macdonald (Eds), *Cyberterrorism* (Springer 2014).

[417] Estonia, *Criminal Code*, § 237.

[418] EU, *Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision* (n 404), § 1.11.

[419] On the inclusion of cyber attacks under the UK terrorism offence see S. Macdonald, 'Cyberterrorism and Enemy Criminal Law' in C. Finkelstein, J. David Ohlin and K. Govern (Eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015), 58ff.

[420] UK, *Terrorism Act 2000*, s 1 (2)(e).

[421] *Id.*, s 1 (1)(c).

to do so. Moreover, it merely must be intended to "influence" a government or an international governmental organisation, or even to "advance" a political, religious, racial or ideological cause.

Both cyberterrorism provisions represent the peak of the criminal repression of cyberattacks. However, they place the *discrimen* between the various degrees of criminalisation on the intent sustaining the cyberattack[422], rather than on the scale and effect of the attack. Neither norm requires that the attack has specific targets, such as critical infrastructures. The material threshold of seriousness envisaged is interference or hindrance (Estonia) or serious interference or disruption (UK) with computer systems.

Considering that both systems envisage an ordinary offence of interference with computer systems, their differentiation between common cyberattacks and cyber terrorism is mostly based on a "terrorist intent".[423] However, the nature of the "terrorist intent" appears diluted when compared to international standards. In particular, the UK provision creates the substantial risk of covering the majority of politically motivated cyberattacks. Even non-terroristic attacks could indeed be "made for the purpose of advancing a political, religious, racial or ideological cause".

This shows that the enactment of specific cyberterrorist offences may be less effective in protecting the principle of *proportionality* and *ultima ratio* than relying on the traditional non-specific terrorist offences.

In light of this analysis, it is important to underline the pivotal role that the legal interest involved plays in deciding upon punishment for cyberattacks. In the case of cyberterrorism, the legal interests protected are not limited to the functioning of a computer system. When cyber terrorism offences

---

[422] Interestingly though, the UK Computer Misuse Act 1990 (CMA) was recently amended by the 2015 Serious Crime Act. Two important amendments aimed to transpose into UK law the provisions of Articles 7 and 12 Directive 2013/40/EU. Section 42 Serious Crime Act amended section 3A of the 1990 Act to include an offence of obtaining a tool for use to commit an offence provided by section 1, 3 or 3ZA offence CMA, removing the prior requirement of involvement (or intended involvement) of a third party (the individual obtained the tool with a view to its being supplied for use to commit the offence). Section 43 extended the extra-territorial jurisdiction of the CMA offences by including the active nationality principle in the categories of 'significant link to the domestic jurisdiction' (section 5 1990 CMA). Moreover, the Serious Crime Act created a new offence of unauthorised acts causing, or creating risk of, serious damage (section 3ZA CMA 1990). The new offence "addresses the most serious cyberattacks, for example those on essential systems controlling power supply, communications, food or fuel distribution" (UK Government, *Serious Crime Act 2015 Fact sheet: Part 2: Computer* misuse <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf>) by prescribing penalties up to life imprisonment for any "unauthorised act in relation to a computer" which causes or creates a risk of serious damage, in the UK or abroad (provided the significant link to the domestic jurisdiction), to the economy, the environment, national security or to human welfare (UK, *Computer Misuse Act 1990*, Section 3ZA (3): For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes: (a) loss to human life; (b) human illness or injury; (c) disruption of a supply of money, food, water, energy or fuel; (d) disruption of a system of communication; (e) disruption of facilities for transport; or (f) disruption of services relating to health). No specific intent is required.

[423] Cfr. G. Fletcher, 'The Indefinable Concept of Terrorism', (2006) 4 Journal of International Criminal Justice 894, 900.

are constructed along the lines of traditional terrorism offences (e.g. French *Code Pénal*, Article 421-1: "*Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes: (…) 2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code*")[424] the concrete judicial evaluation of an effective harm or endangerment to the legal values protected by the terrorist legislation – such as public order or national security – may be an effective dividing line between cybercrime and cyberterrorism.[425]

---

[424] "The following offenses constitute acts of terrorism, when they are intentionally connected with an individual or collective enterprise whose purpose is to seriously disturb public order through intimidation or terror: (2) Thefts, Extortion, destruction, damage and deterioration, as well as computer-related infringements defined in Book III of this Code".

[425] In particular, within legal systems structured on the "*Rechsgut*" theory, a concrete consideration by the interpreter of an effective threat / harm to the legal good involved may be necessary. See for instance the "*principio di offensività*" in the Italian system (*ex plurimis*, IT, Corte Costituzionale, *Judgement n. 263/2010*). On the concept of *Rechtsgut* (legal good), see e g C. C. Lauterwein, *The Limits of Criminal Law: A Comparative Analysis of Approaches to Legal Theorizing* (Ashgate Publishing 2013), 5 ff.

II.VII. DIGITAL CRIMINAL ORGANISATIONS AND TRADITIONAL JOINT CRIME MODELS.

Technological progress, and in particular the development of the Internet, has led to the rise of new criminal phenomena related to the use of digital technologies. Specific problems in applying the traditional substantive and procedural criminal concepts to this type of crime began to occur. Consequently, criminal law has undergone substantial reforms – often stimulated at the international level – aimed at adapting the legal framework to such criminological changes.

In addressing the criminological transformations brought about by the digital revolution, criminal law has heavily relied upon a conception of digital technology as a *place.*[426] Since this place contains legal interests that could be exploited by criminals, it should be protected by the legal order.

Despite the increasing diffusion of social media, Internet fora and community-based interaction, criminal law has given scarce consideration to the social significance of cyberspace as an *anthropological space.*[427] Cyberspace is a place of social aggregation, a digital *agora*. As new technologies permit the remote connection, coordination, and joint action of its users, individuals increasingly gather online to form new social forms of internet-based network organisations.[428] Such organisations, just like those in non-digital reality, may engage in licit or illicit behaviours.

Within the predominant legal discourse, substantial attention is given to the fact that cybercrime does not require the physical proximity between victims and perpetrators.[429] Similarly, if cyberspace is considered in its social dimension, members of the same group hold the capacity to jointly operate online regardless of their geographical location. This may substantially influence the external features and the internal dynamics of the collective at stake. In particular, digital criminal consortia may be composed of members from all over the world, gathering on digital platforms. They may be unaware of each other's personal identity and conduct their interactions exclusively via online chats and fora. The structural features that may characterise such organisations are therefore inherently different from those of traditional criminal consortia. Furthermore, the digital

---

[426] See M. de Certeau, *L'Invention du Quotidien* (Gallimard, 1980).

[427] See M. Merleau-Ponty, *Phénoménologie de la perception* (Gallimard, 1945).

[428] See D. Ronfeldt, *Tribes, Institutions, Markets, Networks: A Framework About Societal Evolution* (RAND Corporation, 1996).

[429] See, *inter alia*, S. Brenner and L. L Clarke, "Distributed Security: A New Model of Law Enforcement", (2005) 23 John Marshall Journal of Computer & Information Law 659, at 666.

social dimension of such an organisation may produce weaker links between the members, influencing the degree of their involvement with its criminal activities.

By relying on the application of traditional joint crime models, cybercrime legislation often falls short of taking into due consideration the peculiar characteristics of cyber interaction. National and international criminal law models of collective crime are usually tailored to traditional (physical) crime. To one or another degree, these models require specific operational and organisational features. Challengingly, new cyber phenomena – and in particular hacker groups – may lack these characteristics. Their structure may be informal and shaped around a virtual space, where operations are planned, or criminal activities are conducted. They may display the features of liquid and amorphous organisms, amenable to the constant entrance and exit of members. The degree of affiliation with the group may vary from a stable association to an extemporaneous participation in the social life of the organism. Furthermore, some internet-based organisations embrace both legal and illegal activities. For instance, in the chatrooms of the renowned hacker collective Anonymous, it is possible to detect the planning of cyberattacks alongside licit social and political activities.

The application of traditional collective crime models to this digital reality is confronted with two main types of problems. First, criminal organisms operating in cyberspace may not meet the operational and organisational requirements of the traditional models. Therefore, the concrete application of such models may either be inefficient or result in their overextension to cover the characteristics of virtual consortia. Given the lack of legislation able to regulate the specific features of virtual groups, States may be tempted to use "exceptional" models tailored to different types of criminal networks. This may entail the risk of inattention to the fundamental principles of criminal law.[430]

Second, the loose structure of online groups, alongside their permeability, may generate issues in terms of defining the limits of individual criminal responsibility for the group's activities. One of the main risks connected to this problem is an excessively broad criminalisation of cybercrime collective phenomena, covering minor participation in the social life of an online organism. In light of the social, economic, and political relevance of many collective digital activities any over-repression of online activities should be avoided.

---

[430] See, on this point, Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Section I – Penal Law. General Part, The Expanding Forms of Preparation and Participation, Final Resolution: "The legitimate status of the fight against terrorism, organized crime and other above-mentioned serious crimes cannot be used as a pretext for an extensive application of exceptional rules. Therefore, every kind of authoritarian tendency must be avoided in the evolution of Criminal Law, ensuring the application of fundamental principles of criminal law, and particularly those of legality, individual culpability, ultima ratio, proportionality and human rights and fundamental freedoms".

This subchapter will analyse the application of traditional models of group crime offences to cyberspace-based criminal collectives. It will use as a focal case-study the politically/ideologically motivated hacker collective "Anonymous". It will then consider the effectiveness of the application of common-law conspiracy doctrines and civil-law criminal association models to this case study. The legal analysis will be combined with socio-criminological findings, related to the operational and morphological characteristics of organised, web-based crime, and to the peculiarities of social and criminal behaviour online.[431] The subchapter will conclude with a brief review of existing case law on crimes perpetrated under the signature of *Anonymous* in order to assess how such models have been applied to online collective networks.

II.VII.VII. A COMPARATIVE PERSPECTIVE ON CRIMINAL INTERACTION AND JOINT CRIME MODELS.

Before embarking in a legal and criminological examination of cyberspace-based criminal collectives, it appears useful to analyse the main conspiracy and criminal association models and their key elements, in order to more effectively evaluate their application on organised cybercrime.

Collective Crime.

Whether acting in the real world or in the digital realm, an individual must be held liable for a crime when he/she engages in a conduct prohibited by a criminal provision (*actus reus*) while having a culpable mind (*mens rea*). Crimes can be committed by a single person, acting alone as the sole perpetrator of the crime, or by a number of persons acting together. The role and the level of involvement of the various individuals participating in a criminal act may vary. However, albeit not every individual behaviour may entirely cover the specific proscribed conduct of the crime, each and every person involved is to be held accountable for the criminal act. The individual conduct of some of the persons involved in a crime may often fail to fulfil the material element of a criminal offence (a classic example is the driver who escorts the robbers to the bank). Hence, the legal need for introducing the concept of *complicity*.

The main function of complicity is to allocate liability to the various actors that collaborated in the crime, even in those cases where their individual conduct does not satisfy the required material

[431] The analysis is based on the review of scientific and journalistic studies on the subject matter as well as a direct sociological observation of the phenomenon and interviews with "hackers" and members of the Cybercrime Agency of the Italian Police Forces.

element. Complicity usually comprises a wide range of participatory behaviours in the criminal offence, from providing substantial aid to encouraging or advising the direct perpetrator(s).[432] Some systems maintain a distinction between principal perpetrators and accessories,[433] although this distinction is of relevance mainly where the system in question provides for a formal difference in terms of punishment.[434]

Notably, the more the criminal interaction between multiple persons acquires stability and structure, the greater the dangerousness of the group. Where individuals are united by an agreement, a promise, or an oath to commit a crime, their criminal will, their force, and their resources are united and strengthened. Such a bond increases their determination to offend and renders the ability of withdraw from criminal plans more difficult.[435] This exponentially augments the potential dangerousness of a group's criminal actions. Collective crimes have proven to be particularly threatening for the legal order and social peace of societies. Legal systems have an interest in countering these consortia at the very moment of their creation and ensuring the liability of each

---

[432] See E. van Sliedregt, *Individual Criminal Responsibility in International Law* (Oxford University Press, 2012), 95ff.

[433] See L. Picotti, 'Expanding Forms of Preparation and Participation - General Report', (2007) 3 Revue Internationale de Droit Pénal 405. Picotti (at 418), distinguishes between "monistic" and "dualistic" systems. The doctrines governing the discrimen between the two categories are various and may be focused on the objective element (mainly followed by the common law systems: the conducts that do not satisfy the material element of the crime, derive their liability from the one of the principal perpetrator, accessing to its crime. Conversely, when the actus reus does satisfy (entirely or some parts of) the material element, the perpetrators are categorized as principals, co-perpetrating in the crime. See A. Ashworth, *Principles of Criminal Law* (OUP, 1999), 426), on the subjective element (see International Criminal Court, *Situation in the Democratic Republic of the Congo, Lubanga Case*, Decision on Confirmation of Charges, ICC-01/04-01/06-803, PTC I, 29 January 2007, § 329 "The subjective approach—which is the approach adopted by the jurisprudence of the ICTY through the concept of joint criminal enterprise or the common purpose doctrine—moves the focus from the level of contribution to the commission of the offence as the distinguishing criterion between principals and accessories, and places it instead on the state of mind in which the contribution to the crime was made. As a result, only those who make their contribution with the shared intent to commit the offence can be considered principals to the crime, regardless of the level of their contribution to its commission"), on the presence of the actors at the commission of the offence (see M. D Dubber, "Criminalizing Complicity A Comparative Analysis" (2007) 5 Journal of International Criminal Justice 977, 981) or on the "dominion or control over the act" (such as in the German and Spanish systems, *Id.*, 981ff; J. Manuel Gómez Benítez, 'El dominio del hecho en la autoría (validez y límites)', (1984) 37 Anuario de derecho penal y ciencias penales 103; J. D. Ohlin, 'Co-Perpetration German Dogmatik or German Invasion?', in C. Stahn (Ed), *The Law and Practice of the International Criminal Court: A Critical Account of Challenges and Achievements* (OUP 2015), 519. See also K. Ambos, *Treatise on International Criminal Law: Volume 1: Foundations and General Part* (OUP 2013), 153).

[434] With regard to punishment, it is possible to notice two main types of approach to the element of participation in the crime. According to the "equivalence" theory, all the individuals participating in the crime are to be punished equally. According to the "difference" theory each participant should be punished according to the degree of his/her participation to the crime, and a distinction is made between perpetrators (or co-perpetrators) and accomplices. See: G. P. Fletcher, *Basic concepts of Criminal Law* (n 143), 188ff. However, the distinction between principals and accomplices can be relevant also with regard to procedural issues. See: M. D Dubber, "Criminalizing Complicity A Comparative Analysis", 892. Cfr Stewart's "unitary theory of participation" in J. Stewart, 'The End of Modes of Liability for International Crimes', (2012) 25 Leiden Journal of International Law 165.

[435] See A. Ashworth, *Principles of Criminal Law* (n 433), 423.

member of the group, notwithstanding their actual role within it (such as, for instance, those who agree to commit a crime but either do not act or act and fail). In particular, this interest arises when the criminal aim of the bond refers to a particularly serious crime, such as crimes against the State or the public order.[436]

In order to promptly curb and punish these collective types of crime, specific typologies of criminal offences have been introduced in criminal law systems.

Expressly, joint crime offences have been enacted for a series of reasons. First, to criminalise the creation of or participation in criminal associations as an autonomous punishable offence from the one committed in furtherance to the agreement (thus having a punishment role). Second, to ensure the liability of each participant in the *societas sceleris,* notwithstanding his/her role (thus having a role of attribution of liability). Third, to offer a strong deterrent by setting the moment of criminalisation at the mere creation of or participation in the group, considered to create a social endangerment even before the actual commission of the predicate crimes (thus having a preventive role).[437]

The main joint crime models: civil and common law.

Traditionally, joint crime offences adopted at the state level are categorised according to two models, ascribing to two historical prototypes: the English *conspiracy* offence and the French *association de malfaiteurs* offence. The conspiracy-type model, which is typically found in common law systems, focuses on the element of the agreement to commit a crime.[438] It emphasises the inchoate function of the offence, since it criminalises the planning of a crime and may not consider necessary an overt act to put the plan into operation.[439] The participation-type, which is the most common model

---

[436] *Id.*, 471ff.

[437] Furthermore, special measures in terms of investigation and prosecution of these collective crimes have been widely introduced in many criminal law systems.

[438] Although the agreement is the *actus reus* of the offence of conspiracy, this is essentially a mental operation (see D. Ormerod, *Smith and Hogan Criminal Law: Cases and Materials* (OUP, 2005), 274.

[439] In this regard, however, common law conspiracy crimes may be divided into two main groups. A first group of countries, such as Canada, England and Wales, and South Africa, does not require any further element in addition to the agreement between at least two persons to commit a crime. Other common law systems, instead, require some additional elements besides the agreement to commit a crime. US, *United States Code*, Title 18, § 371, for instance, requires that "… one or more of such persons do any act to effect the object of the conspiracy…" (See also, *inter alia*, US, *United States of America v. Conti, 804 F.3d 977, 979-80* (9th Cir. 2015); US, *United States of America v. Ngige*, 780 F.3d 497, 503 (1st Cir. 2015); US, *United States of America v. Salahuddin*, 765 F.3d 329, 338 (3d Cir. 2014). However, other federal statutes on conspiracy do not foresee an explicit overt act as a requirement. For instance, see US, *United States v. Pascacio-Rodriguez*, 749 F.3d 353, 361-362 (5th Cir. 2014)) In any cases, the overt act needs not to be the substantive crime, which is the object of the conspiracy, or an unlawful act. It merely requires to be a "step towards the furtherance of the criminal plan" (see, *ex plurimis*, US, *United States v. Rehak*, 589 F.3d 965, 971 (8th Cir. 2009)).

across civil law systems, is instead centred on the element of a structured organisation, created through the *pactum sceleris* and on the criminalisation of the "participation" in the criminal consortium.

The element that triggers the criminalisation is thus different in the two models. In the conspiracy doctrine, the structural *discrimen* between the simple attribution of liability and autonomous criminalisation rests solely on the formal or tacit stipulation of a criminal agreement between the parties. It therefore focuses on the existence of a conspiratorial relationship aimed at the commission of crimes. Notwithstanding its possible occasional and extemporaneous nature, the mere agreement to commit a crime is criminalised as an autonomous offence, "a distinctive evil which may be punished whether or not the substantive crime ensues"[440] (and eventually combines with it).

Conversely, in civil law systems, the element that triggers criminalisation is the nature of the social organism created by the agreement. The participation model justifies the autonomous criminalisation of the participation in the group only *vis-à-vis* the creation of a structured and stable organisation. Through such a structure, the meeting of the will, strength, and resources of the members, and the coordination between them, substantially endanger the social order and the specific legal interests eventually touched by the criminal plans of the organisation. This consideration is in line with the general principles of criminal law (and in particular, the principles of legality, individual culpability, *ultima ratio*, and proportionality). As pointed out by the *Association Internationale de Droit Penal* in its XVIII Congress, "the criminalization of association and organization as a separate crime requires that objective and subjective elements of the offence are precisely described, such as its stability, the fact that it might constitute a durable danger for a certain time period, its structure, and possibly characteristic acts (modus operandi: like use of violence, or mafia method, etc.)."[441]

This twofold approach is mirrored in the main international instruments on organised crime. However, these instruments suggest a substantial level of equivalence between the two models. The

---

[440] US, *United States v. Jimenez Recio*, 537 US 270, 274 (2003).

[441] The concept of conspiracy is not completely foreign to civil law systems. However, in these systems a simple and extemporaneous agreement to commit a crime is usually criminalised only when the crime(s) planned by the group poses a threat to particularly important legal interests, such as public order or national security. This is the case, for instance, of the French "*complot*" offence, (FR, *Code Pénal,* Art. 412) limited to "*actes de violence de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national*" (acts of violence likely to endanger the institutions of the Republic or to undermine the integrity of the national territory), or the Italian political conspiracy offence, "*Cospirazione politica mediante accordo*" (ITA, *Codice Penale,* Art. 304), limited to crimes "against the personality of the State". Nonetheless, these offences, whereas they do not merge with the predicate offence in case this is completed, mainly have a preventive function and not an aggravating one. See L. Picotti, 'Expanding Forms of Preparation and Participation - General Report' (n. 433), 418.

EU Instruments on organised crime (Joint Action 733 of 1998 and Framework Decision 841 of 2008) and the UN Convention against Transnational Organized Crime (the 2000 Palermo Convention) allow States parties to choose between the two models as well as to use both.[442]

However, this dichotomy is far from being absolute. A comparative analysis of the various criminal systems readily indicates a varied panorama of tools used to address organised crime. Furthermore, it reveals a vast array of nuances of adherence to one or another model.[443] The traditional *discrimen* between the models seems to have lost a substantial proportion of its relevance, as the application of the two models within national criminal law systems has resulted in convergence. [444] Such a process seems to have occurred not so much out of attention to the "shield", i.e. the interest of the defendant, but in order to ensure an effective "sword" to punish perpetrators and generate credible disincentives.

The conspiracy model, which in the legal discourse has received ample critique related to its vagueness,[445] appears unable to cover the activities of large, multi-faceted criminal enterprises. The use of conspiracy offences is burdened by the necessity to prove that the members of groups are parties to the same agreement. This model can also be inefficient in covering decentralised groups acting under the umbrella of the same organisation, or ensuring the liability of participants in the organisation who are not part of the agreement.[446] Therefore, several common law systems have

---

[442] See F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 26ff. As an example, the Palermo Convention (UN, *Convention against Transnational Organized Crime and the Protocols Thereto*, adopted by the UN General Assembly by Resolution A/RES/55/25, 15 November 2000) at Article 5, requires parties to establish either or both the two types of criminal organisation offences, autonomously "from those involving the attempt or completion of the criminal activity". Namely, the two offences are: "agreeing with one or more other persons to commit a serious crime for a purpose relating directly or indirectly to the obtaining of a financial or other material benefit and, where required by domestic law, involving an act undertaken by one of the participants in furtherance of the agreement or involving an organized criminal group"; and taking an active part, "with knowledge of either the aim and general criminal activity of an organized criminal group or its intention to commit the crimes in question" in the "criminal activities of the organized criminal group" or in "other activities of the organized criminal group in the knowledge that his or her participation will contribute to the achievement of the above-described criminal aim". Furthermore, the Article envisages the criminalisation of abetting, facilitating or counselling the commission of serious crime involving an organised criminal group (thus, the accessorial liability for "external" complicity in the criminal activities of the group), or organising and directing the group.

[443] It should be noted that many systems provide for various types of group offences, which may tend towards one or the another type of model, thus offering to the prosecutor a range of options under which subsuming a collective crime. For instance, the Canadian criminal code envisages both a conspiracy and a participation in a criminal organisation offence.

[444] See J. Okoth, *The Crime of Conspiracy in International Criminal Law* (Springer 2014), 201.

[445] See Note, 'The Conspiracy Dilemma: Prosecution of Group Crime or Protection of Individual Defendants', (1948)62 Harvard Law Review 276, 276- 277. See also US, *Krulewitch v. United States,* 336 US 440 (1949); US, *Harrison v United States,* 7 F2d 259 (2d cir 1925).

[446] See M. Levi, A. Smith, *A comparative analysis of organised crime conspiracy legislation and practice and their relevance to England and Wales* (Home Office Online 2002), 3 <http://library.college.police.uk/docs/hordsolr/rdsolr1702.pdf>.

adopted specific offences more oriented towards criminal association. In 1970, the US enacted the Racketeer Influenced and Corrupt Organizations (RICO) Act, which is not focused on the agreement, but rather on the "pattern of racketeering activity" committed in relation to a "criminal enterprise".[447] In 1997, Canada enacted an offence of participation in a criminal organisation "composed of three or more persons" and not including "a group of persons that forms randomly for the immediate commission of a single offence".[448] In 2015, the UK created the offence of participating in the activities of an organised crime group, defined as a "group that has as its purpose, or as one of its purposes, the carrying on of criminal activities, and consists of three or more persons who act, or agree to act, together to further that purpose."[449]

In contrast to this, the traditional civil-law model has often proved too narrow to combat new types of criminal organisations, which may present different *modi operandi* and softer organisational features from the ones required by this model. Following criminological evolution, some systems have undergone a substantial dilution of the material elements of their criminal association offences. The French *association de malfaiteurs* was originally formulated to cover the structure of banditry and required a rather strong hierarchical structure.[450] As a result of criminological evolution, and particularly the need of combating non-hierarchical anarchist groups towards the end of the 19th century,[451] the offence lost most of its structural elements, and substantially converged in the direction of the criminalisation of "conspirational agreements."[452] Analogously, the Italian *associazione per delinquere* has been interpreted by judges according to the empirical modification of the types of criminal association, and has thus progressively evolved to cover softer structural characteristics.[453]

Furthermore, several civil law systems have opted for a diversification of criminal organisation offences according to operational traits, to the predicate crimes, or to the organisational elements.[454] This is true in the case of the Italian *associazione di stampo mafioso*, but also in the case of the widely

---

447 See G. R. Blakey and B. Gettings, 'Racketeer Influenced and Corrupt Organizations (RICO): Basic Concepts – Criminal and Civil Remedies', (1980) 53 Temple Law Quarterly 1009. See also US, *United States Code*, Title 21, § 848 - Continuing criminal enterprise, on organized narcotics criminality.

448 Canada, *Criminal Code*, § 467.1.

449 UK, *Serious Crime Act 2015*, § 45.

450 FR, *Loi du 12 Fev. 1810,* 11 Bulletin des Lois n. 277bis at 1 (1810). F. Pardo, *Le groupe en droit penal* (PAR, 2009), at 159. See also C. Chanteret, *Le crime des association de malfaiteurs* (Waltener et Cie, 1912).

451 F. Pardo, *Le groupe en droit penal* (n 450), 160.

452 *Id.,* 161-163. See also, C. Elliott, *French Criminal Law* (Routledge 2001), 102.

453 See G. De Francesco, '*Gli artt. 416, 416 bis, 416 ter, 417, 418 c.p.*', in P. Corso, G. Insolera and L. Stortoni (Eds), *Mafia e criminalità organizzata* (UTET 1995), 10.

454 See, on an overview of the European Panorama, F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 55ff.

diffused terrorist association offence.[455] Worth noting for the purpose of this work is the fact that, in the case of a diversification of the structural element, sanctions have often been scaled according to the structure and stability of the group. Such graduation follows the underlying principle that a tighter structure expresses higher social danger. Examples are to be found in the French and Spanish systems. The French system – aside from the *association de malfaiteurs* offence (Art. 415-1 *Code pénal*) – envisages an aggravating circumstance of *bande organisée*. Notwithstanding the same normative formulation of Art. 415-1 with regards to the structural element ("*tout groupement formé ou toute entente établie*")[456], according to the French Supreme Court "*la bande organisée suppose la préméditation des infractions et, à la différence de l'association de malfaiteurs, une organisation structurée entre ses membres.*"[457] The Spanish criminal code foresees three different criminal organisation offences: first, an offence of *asociation illicita*, which requires the existence of a stable and complex organisation[458]; second, an offence of *organización criminal*[459], which covers stable groups acting within a framework of coordination and with a division of tasks and functions[460]; and third, an offence of *grupo criminal*[461], aimed at the repression of criminal groups whose structural organisation lacks all or some of the material requirements of the *organización criminal* offence[462].

---

455 See, for instance, Belgium, *Criminal Code*, Article 139-141, which defines terrorist groups as "*l'association structurée de plus de deux personnes, établie dans le temps, et qui agit de façon concertée en vue de commettre des infractions terrorists*" (The structured association of more than two persons, established over time, acting in a concerted manner to commit terrorist offenses).

456 "Any formed group or any established agreement".

457 FR, Cour de cassation, Chambre Criminelle, 8 juillet 2015, *n° de pourvoi 14-88329* ("The '*bande organisée*' implies the premeditation of the offenses and, unlike the '*association de malfaiteurs*', a structured organization between its members").

458 See Spain, Tribunal Supremo, *STS 20/01/2009, STS 25/11/2008*. On the problems related to the distinction between *organizacion criminal* and *association illicita*, see J. M. Suárez López, 'Aspectos dogmáticos y político criminales en el tratamiento penal de la delincuencia organizada', (2012) 30 Anales De Derecho 90.

459 See Spain, *Codigo Penal*, Art. 570bis (*Ley Organica 5/2010*). See also J. L. De la Cuesta-Arzamendi, 'Tratamiento de la delincuencia organizada en España: en particular, tras la reforma penal del 2010', (2013) 55 Revista Criminalidad 81.

460 "*A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos, así como de llevar a cabo la perpetración reiterada de faltas*" (For the purposes of this Code, "organización criminal" means a group consisting of more than two persons of a stable nature, or established for an indefinite time, who in a concerted and coordinated manner distribute various tasks or functions in order to commit felonies, as well as to carry on the repeated perpetration of misdemeanors).

461 See Spain, *Codigo Penal*, Articulo 570ter. See also Spain, Fiscalia General Del Estado, *Circular 2/2011 sobre la reforma del código penal por ley orgánica 5/2010 en relación con las organizaciones y grupos criminals* (2011).

462 "*A los efectos de este Código se entiende por grupo criminal la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas*" (For the purposes of this Code, "grupo criminal" means the union of more than two persons who, without meeting any or some of the characteristics of the "organización criminal" defined in the preceding Article, have as their object or purpose the concerted perpetration of felonies or the concerted and repeated commission of misdemeanours).

The requirements of a criminal organisation: structure, stability, and additional elements.

A comparative analysis highlights a varied set of joint crime offences, which substantially differ according to the material element.[463] The main elements of differentiation between joint crime offences are the organisational traits of the group, its temporal stability, its modus operandi, its specific goal or features, or the type of planned offences (predicate crimes).[464]

The level of organisation required can range from no requirement of a structured hierarchy – for instance, in the conspiracy-type models or in the French *association de malfaiteurs* – to a hierarchical structure with a set division of tasks, such as in the Spanish *organización criminal* or in the German *Bildung krimineller Vereinigungen.*[465] The stability of the group is also variously considered. Stability requirements stretch from a merely occasional agreement in the conspiracy models, to almost permanent groups, such as in the Austrian offence (§278a *Strafgesetzbuch*, "*auf längere Zeit angelegte*")[466].

At the international level, the main instrument on organised crime provides for a soft structural requirement, delineated *ex negativo*. The UN Palermo Convention defines an "organized criminal group" as a "structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention". However, the instrument specifies that a "structured group" must be intended as "a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure". Such a definition is substantially reprised by the EU instruments on the fight against organised crime.

Furthermore, joint crime offences may require specific *modi operandi*, such as the use of violence or intimidation (as seen in Italian Mafia-type organisation: "*l'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti*")[467]. In other cases, it is the criminal aim of the organisation that constitutes a defining requirement, such as the requirement in the UN Palermo Convention that the group must: "commit a serious crime for a purpose relating directly or indirectly to the

---

463 See, F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 68ff.

464 Another constitutive element is the number of participants, whose minimum can be two, three, or four. See F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 69.

465 See J. Okoth, *The Crime of Conspiracy in International Criminal Law* (n 444), 54; T. Fischer, "§ 129, Bildung krimineller Vereinigungen", in *Strafgesetzbuch und Nebengesetze* (Beck 2012).

466 "Established over a long period of time".

467 ITA, *Codice Penale*, Art. 416 bis. "The association is of the mafia type when the members avail themselves of the intimidating power of the associative bond and of the condition of subjection and omertà to commit crimes".

obtaining of a financial or other material benefit", or in Article 324bis of the Belgian Criminal Code, which specifies that crimes must be carried out "*pour obtenir, directement ou indirectement, des avantages patrimoniaux*")[468].

Finally, the offence can be applicable to any criminal group regardless of the type of predicate offence they have committed or are planning to commit, or conversely may have quantitative (calibrated on the amount of penalty of the predicate offence) or qualitative requirements (only certain types of predicate crime).

II.VII.VIII.CRIMINAL INTERACTION IN CYBERSPACE: IS IT "ORGANISED" CYBERCRIME?

The lack of specific organised cybercrime offences.

The ultimate aim of a legal system is to regulate the social phenomena through which society expresses itself and to sanction its criminal deviations. If we agree that "a crime is a prohibited behaviour", we also acknowledge a precise temporal path: a particular type of behaviour is observed, analysed, deemed undesirable or dangerous to society, then typified in a provision that describes it. Finally, once the offence is adopted and shared by the community, the behaviour is actively criminalised. Criminalisation is designation.[469]

The criminal provision is a verbal speculum of this behaviour,[470] depicting it with sufficient accuracy so as to give a precise command and directing the conduct of citizens. Every criminal offence is thus preceded by a criminological consideration, which sheds light on the type of behaviour that should be prohibited.

As demanded by the principle of legality, substantive criminal law should delineate with sufficient precision what types of behaviour should be prohibited and, when committed, sanctioned. A narrow criminal organisation offence, which is well constructed on an attentive socio-criminological analysis of the phenomena it wishes to combat, reduces the risk of violating the general principles of criminal law aimed at "shielding" the citizen from an excessive use of the *ius punendi*, providing them with better guidance on how to (legally) behave. Nonetheless, a narrow definition bears the risk of decreasing its effectiveness to cover emerging forms of organised crime.

---

468 "To directly or indirectly obtain a financial gain".

469 See, e.g., G. P. Hoefnagels (Ed), *The Other Side of Criminology: An Inversion of the Concept of Crime* (Springer Science & Business Media 2013), 92.

470 See M. Papa, *Fantastic voyage: Attraverso la specialità del diritto penale* (Giappichelli 2019).

Mirroring the social, political, and financial changes within modern societies, criminal organisations have developed in various forms: banditry, national mafia-type organisations, transnational narcotics organisations, domestic political terrorist groups, international religiously-motivated terrorist organisations, etc. [471] The analysis of this phenomenon has mainly focused on specific "phenotypes" of collective criminality which were active within a given space throughout a given time. Clearly, these phenotypes possess different features. The Italian Mafia presents different traits from organised banditry in the Horn of Africa, or from hacker groups. Accurate depiction of these types of criminality leads to different criminological models, which translate into inherently different norms, able to cover only specific forms of joint crime. Conversely, any attempt to reduce criminological precision to a unique model necessarily dilutes its adherence to the criminological reality. Instead of focusing on precise criminal behaviours, expressing particular traits of dangerousness, such model covers all criminal aggregations of persons.[472]

In order to cover the shape-shifting nature of criminal organisations, criminal systems have reacted to the diachronic evolution of organised criminality in two ways. In some cases, they have diluted the constituent element of the crime, sacrificing criminological preciseness and adherence to the peculiar traits of the phenomenon, and expanding the scope of the offence. In other cases, they have enacted new offences, providing for a set of differentiated tools aimed at accurately targeting different criminal realities. For instance, new joint crime offences have been enacted in order to cover mafia-type organisations and terrorist groups.

Despite the increasing relevance that cyber interaction and cybercrime are acquiring in modern societies, no specific offence has yet been enacted to cover the specificities of cybercriminal organisations – i.e. criminal phenomena that are exclusively formed and active online. This issue is scarcely addressed at either the domestic or the international level. International criminal instruments – usually at the forefront in providing for effective regulations on cybercrime issues – have not yet demonstrated much attention to the organisational and operational features of hacker groups. Nor have they provided for any specific offence on the issue. The CoE Convention on Cybercrime merely calls for States Parties to "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences (…) contained in the Convention with intent that such offence be committed."[473] The EU Instruments on attacks against information

---

[471] See, inter alia, C. Fijnaut and L. Paoli (eds), *Organized Crime in Europe* (Springer 2006), 21ff.

[472] These observations are undoubtedly generally applicable to law: what is gained in specificity is inevitably lost in scope (and thus in "effectiveness").

[473] CoE, *Convention on Cybercrime* (n 81), Article 11.

systems do envisage the aggravating circumstance of committing the listed offences within the framework of a criminal organisation. However, they rely on the definition given by the EU Joint Action[474] and in its replacing Framework Decision on the fight against organised crime[475]. These provisions were widely implemented into States Parties' criminal law, either by providing for a specific aggravating circumstance (e.g. Estonian, German or Austrian cybercrime laws provide for the aggravating circumstance of committing cybercrime from within a criminal organisation), or indirectly, through the application of the ordinary provisions on traditional criminal organisations.[476]

At the domestic level, only France has enacted a specific provision criminalising digital criminal consortia (*association de malfaiteurs informatique*)[477]. However, the offence is modelled on the traditional *association de malfaiteurs* offence. In fact, the main aim in creating a new cyber specific offence was to overcome the quantitative threshold of the predicated crimes contained in the traditional association offence (thus being able to cover associations aimed at committing cyber offences punishable with lesser sanctions). The *association de malfaiteurs informatique* offence does not require any specific organisational or operational requirements. Furthermore, its judicial application was criticised as operating a further dilution of the structural element of association, covering acts that could be better classified as complicity.[478]

Interestingly, Law n° 2014-1353, "*renforçant les dispositions relatives à la lutte contre le terrorisme*", introduced into the French Penal Code the aggravating circumstance of committing cyber offences against public computer systems (Articles 323-1 to 323-3-1 *Code Pénal*) within the framework of a criminal organisation.[479] The aggravating circumstance, however, is not based on the *association de malfaiteurs informatique*, but on the notion of *bande organisée*. It thus requires a more complex structural organisation than the offence of *association de malfaiteurs informatique*.

The general trend that can be observed is that the fight against organised cybercrime still relies on those offences enacted on the basis of traditional collective crime models, and that the peculiar criminological features of organised cybercrime have usually been disregarded. The absence of

---

474 EU, *Joint action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (98/733/JHA)*, OJ L 351, 29.12.1998.

475 EU, *Council Framework Decision of 24 October 2008 on the fight against organised crime (2008/841/JHA)*, OJ L 300, 11.11.2008.

476 EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* (n 148), 7-8.

477 FR, *Code Pénal,* Article 323-4.

478 See A. Lepage, P. Maistre du Chambon and R. Salomon, *Droit Penal des Affaires* (n 249), 264. See also France, Cour d'Appel de Aix-en-Provence, 2 juin 1993.

479 FR, *Code Pénal,* Article 323-4-1.

specific cybercriminal organisation offences evidently rests on the consideration that organised cybercrime consortia present similar features to traditional organised criminal groups.[480]

While on the surface hacker groups may present some similarities to traditional criminal organisations, when studied with accuracy they present distinctive features that are not easily captured by the existing models.

However, such a conclusion may be drawn with regard only to those organised criminal groups that are formed and that operate exclusively through digital means. Indeed, their morphology and *modi operandi* are necessarily affected by the dynamics that characterise the digital space in which they operate. The same observation does not apply to the traditional organised criminal groups that have online ramifications and are actively engaged in cybercriminal activities.[481] Clearly, the organisational features of this latter group are likely to remain unaltered and their structured and stable hierarchical organisation is reflected in their online manifestations.[482]

When is a crime "organised"?

In order to assess whether and to what extent existing criminal organisation offences fit organised cybercrime, it is useful to consider the main criminological constituent elements of these traditional offences.

Existing criminological illustrations of organised crime usually emphasise the relevance of the aims and the operational features of the group. The most frequently observed aim of traditional organised criminal groups is the economic nature of the crime,[483] and a series of particular *modi operandi*, such as the use of corruption, violence, intimidation, or secrecy to further their criminal

---

480 See S. Zambo, 'Digital La Cosa Nostra: The Computer Fraud and Abuse Act's failure to punish and deter organized crime', (2007) 33 New England Journal on Criminal and Civil Confinement 551.

481 See K. R. Choo, 'Organised crime groups in cyberspace: a typology', (2008) 11 Trends in organized crime 270, 271ff. See also R. G. Smith, 'Transnational Cybercrime and Fraud', in P. Reichel and J. Albanese (eds), *Handbook of transnational crime and justice* (Sage 2013), 121-122.

482 The power structure of a criminal organisation appears hierarchical where the specialisation of group roles and a stable membership reduce its permeability to the fluid entering and/or exiting of individuals. See D. Luban, J. R. O'Sullivan and D. P. Stewart, *International and Transnational Criminal Law* (Aspen 2010), 505.

483 See H. Abadinsky, *Organized Crime* (Wadsworth Publishing 2010), 3; J. E. Conklin, *Criminology* (Pearson 2007), 315; P. Beirne and J. W. Messerschmidt, *Criminology* (OUP 2006), 160; J. S. Albanese, *Organized Crime in America* (Anderson Publishing 1989), 4-5. See also Federal Bureau of Investigation, *Organized Crime* <https://www.fbi.gov/investigate/organized-crime>.

aims.[484] Reflecting these models, many joint crime offences contain these features as constituent elements of the crime.[485]

However, the constant evolution of collective crime and the wide diffusion of transnational criminal groups may lead to de-contextualising these specific criminological descriptions from reality. As previously pointed out, in enacting or applying these criminal organisation offences most States either rejected the specific aims or *modi operandi*,[486] or envisaged – besides the narrower definitions – more general and "a-specific" offences.[487]

The primary constituent elements of such general offences are the organisational features of the group and its stability.[488] These elements are the core of any joint crime offence. From a criminological point of view, their role is important in terms of distinguishing organised crime from extemporaneous criminal interaction (such as, for instance, protesting and rioting). From a legal point of view, they distinguish joint crime offences from ordinary modes of liability and inchoate crimes such as complicity and attempt, and justify their prevention and punishment role.

The organisational traits of the group are the elements that permit the coming together of the will, strength, and resources of the various members. From this gathering originates the "autonomous" collective power of the group (as a sort of "super-organism"), which allows the criminal entity to be more effective in committing crimes than the mere sum of the individuals would be if acting alone. Such a criminal collective begins to present a social danger that goes beyond the danger expressed by its various components.[489] The risk that criminal consortia pose to the legal order grows

---

[484] See D. N. Falcone, *Dictionary of American criminal justice, criminology, and criminal law* (Pearson/Prentice Hall 2005), at 187; Robert Rhodes, Organized Crime: Crime Control vs. Civil Liberties (Random House, 1984), at 4.

[485] For example, the UN Palermo Convention's provision provides for the requirement of the group's aim of obtaining "directly or indirectly, a financial or other material benefit" (UN, *Convention against Transnational Organized Crime and the Protocols Thereto (*n 442)); Austria, *Strafgesetzbuch*, Article 278a covers an association "*die dadurch eine Bereicherung in großem Umfang anstrebt; und die andere zu korrumpieren oder einzuschüchtern oder sich auf besondere Weise gegen Strafverfolgungsmaßnahmen abzuschirmen sucht*" (that tries to gain a large enrichment through the above mentioned crimes; and that corrupts or intimidates others or tries to protect itself from prosecution); Swizerland, *Criminal Code*, Article 260ter punishes participation in a "*organisation qui tient sa structure et son effectif secrets et qui poursuit le but de commettre des actes de violence criminels ou de se procurer des revenus par des moyens criminels*" (Any person who participates in an organisation, the structure and personal composition of which is kept secret and which pursues the objective of committing crimes of violence or securing a financial gain by criminal means).

[486] See Israel bill introducing the 2003 Combating Criminal Organization Law, which specifically rejects financial or material benefits in order to "not limit the objectives of the organization, so that it may also include other objectives, such as ideological objectives" (see B. Sangero, 'Are All Forms of Joint Crime Really 'Organized Crime'? On the New Israeli Combating Criminal Organizations Law and Parallel Legislation in the US and Other Countries," (2007) 29 Loyola of Los Angeles International and Comparative Law Review 61.

[487] See for instance, the Italian offences of "Associazione per delinquere" (Art. 416, *Codice Penale*) and "Associazione di tipo mafioso" (Art. 416 bis, *Codice Penale*).

[488] See also J. L Albini, *The American mafia: Genesis of a legend* (Appleton-Century-Crofts 1971), 35ff.

[489] See See L. Picotti, 'Expanding Forms of Preparation and Participation - General Report' (n 433), 414.

according to the level of its organisation. This level depends mainly on the quality of its coordination and communication mechanisms, the strength of cohesion, and the stability of the group.

The ability to act in an organised way is undoubtedly the *discrimen* between a crowd and a criminal association. One of the key variables in the organisation of a group is thus the ability of the members to coordinate their intentions and – using the words of the Palermo Convention – act "in concert". As observed by Jens Ohlin, "if individuals pursue the whole plan independently of each other, the result is hardly a conspiracy. It would be nothing more than multiple individuals who happen to be working toward a similar goal, but without any effective coordination of their activities. This is the opposite of a conspiracy. This is more like crowd behaviour: independent actions that happen to lead to an aggregate result."[490] Through interactive synergy between members, the group increases its efficiency. Concerted actions allow the different participants to be more effective in reaching their goal than the mere sum of their individual actions. At the very basis of a group's coordination lies communication, through which the members transmit and receive information on each other's intentions, formulate orders, and take or disclose decisions.

In large groups, coordination necessarily relies on structural designs, which allow direct decisions, communication flows, and division of labour. Such structural designs can be primarily categorised as vertical or horizontal. A vertical organisation of the group is based on an internal hierarchy, with clearly defined roles and tasks. The roles and tasks may be allocated *ex ante,* deriving from a primordial foundational moment. There, the fundamental traits of the hierarchical structure are formalised and institutionalised. Each new member will be introduced to this structure. His or her role and task will thus become a necessary element of the *pactum sceleris* which links the group's members, assigns them a position within the group, and allows them to coordinate and provide their contribution to reach the final goal. In vertical structures, the upper level decides the aim, the common plan envisaged to pursue it, and the various roles of the participants. The decisions are then communicated to the subordinates through a command and control system, which links the participants of the group and provides for a precise coordination of members' actions.[491]

A division of tasks and roles may also derive from a horizontal deliberative structure. Outside of any interaction based on command and control between superiors and subordinates, such a structure decides the aim of the group and coordinates the participants towards it. Duties and tasks are not

---

[490] See J. D Ohlin, 'Group Think: The Law of Conspiracy and Collective Reason', (2007) 98 Journal of Criminal Law and Criminology 147, at 178. See also P. French, *Collective and Corporate Responsibility* (Columbia University Press 1989), 68.

[491] See generally R. Mousnier, *Social hierarchies, 1450 to the present* (Schocken 1973); E. O. Laumann, P. M Siegel and R. W. Hodge (eds), *The logic of social hierarchies* (Markham 1970).

institutionalised according to status or authority. Rather, they are allocated through an *inter pares* decision-making structure, which defines the way in which the actions of the participants are coordinated. Coordination is provided for exclusively by the deliberation between pairs, without any hierarchy of rulers or superiors. However, a high number of members will likely decrease the efficiency of a horizontal decision-making structure. The more peers participate in a discussion, the harder it will be to reach an agreement.[492]

In the lack of a unitary chain of vertical command, decentralisation is often used to facilitate coordination between large groups. This is true in the case of Al-Qaeda and of the European political terrorism of the 1970s. Decentralised structures, however, require coordination both within a sub-section (a node or a cell), and among sub-sections. The link between subsections reflects, therefore, the same coordinative problems as organisation within of a group of individuals. In particular, the lack of coordination between the nodes negates any existence of a superstructure, considered as a unitary entity overarching the nodes. Again, the needs for directing the work of the network may require the existence of some sort of vertical structure. Currently, formal hierarchy is typical of many criminal organisations. Conversely, it is hard to find any cases of purely horizontal organisation structures in large criminal groups. Most decentralised groups usually present a hybrid structure, with both vertical and horizontal features. For instance, decentralised systems may envisage a horizontal structure of organisation in smaller sub-nodes, but encompass a directive leadership to coordinate those nodes. [493]

Another pivotal element that defines a criminal organisation is its internal cohesion. As an agglomerate of molecules forming an organism, the cohesion of its members defines the group's collective identity. Clearly, along with coordination, the quality of interaction is based on the "rational" [494] unity of the group and on the stability of membership. This implies the reduction of the personal autonomy of its members, for the sake of pursuing a collective criminal aim. The more separate the will of the whole group from those of its individual members, the more those members will be prone to abandoning their personal inclinations in order to follow the criminal plan.

The bond between the individual and the group is often initially created by a mutual agreement between new members and the collective. Such an agreement is composed, on the one hand, by the

---

[492] Digital technology may strongly facilitate communication between networks having high numbers of members, since it rationalises the outcome of multi-actors' communication. Indeed, it plays a fundamental role in enabling horizontal structuration in many new organisational phenomena, such as new direct democracy-based political parties.

[493] See, with regards to Islamic terrorism, C. Dishman, 'The Leaderless Nexus: When Crime and Terror Converge', (2005) 28 Studies in Conflict & Terrorism 237; J. Arquilla and D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Rand Corporation 2001). See also, with regards to Brigate Rosse in Italy, S. Quirico, 'Il modello organizzativo delle Brigate Rosse in una prospettiva comparata' (2008) 44 Quaderni di storia contemporanea 1, 3.

[494] See J. D Ohlin, 'Group Think: The Law of Conspiracy and Collective Reason' (n 490). 180.

will of individual members to participate in the collective, and to adhere to its plan. On the other hand, it includes the approval of the rest of the group.[495] This initial *pactum sceleris* sets out the position and the role of the joining party. With it, the member accepts to follow a set of rules, and to work in pursuance of common goals, pledging loyalty to the criminal plan.

The relationship between the individual and the group has to be actively and constantly corroborated throughout the various activities of the collective. The "unitary will" of the collective is ensured by mechanisms of accountability. In particular, accountability of individual members needs to be supported by a credible system of control, adjudication, and enforcement of sanctions in cases of non-compliance.

Cohesion of a group permits the consideration of the collective body as an autonomous entity persistently engaged in its activities over time. The relation between the member and the group's rational unity works as the legal link between the individual's culpability and liability for participating in a criminal group.

The final element that distinguishes a criminal organisation from other extemporaneous and less dangerous criminal activities (usually limited to the commission of only one offence) is its temporal stability.[496] The requirement of a continuous duration of the organisation is envisaged by numerous legal systems.[497] It indicates the will of the State to exclusively target associations which aim at the prolonged commission of criminal activities, and pose a continuous (and, in some cases, permanent) danger to the legal interests of the social order, and the ones specifically affected by the predicate crimes.

The stability of the group, however, should also be intended as its continuity or self-perpetuation.[498] The group's activities and existence must continue beyond the social life of its members. The composition of the group may change over time; members can be arrested or replaced. Yet this must not affect the group's existence or its criminal plans. The continuity of the group is thus diametrically opposed to that of its members. As pointed out (*inter alia*) in the Palermo Convention, the group "does not need to have (…) continuity of its membership".

---

[495] See, for instance, the "initiation rituals" in the Italian Mafias (*inter alia* S. Strati, "Il Codice della 'Ndrangheta'" (1992) 26 Forum Italicum: A Journal of Italian Studies 281).

[496] See F. Calderoni, *Organized Crime Legislation in the European Union* (n 159), 74.

[497] In particular, in the civil-law criminal association models.

[498] See J. O. Finckenauer, 'Problems of definition: what is organized crime?' (2005) 8 Trends in organized crime 63, 66.

II.VII.IX. LITMUS TEST FOR ORGANISED CYBERCRIME: THE ANONYMOUS CASE.

A group, a collective, or a network?

The existing organised cybercrime scenario is composed of various cyber-actors, which differ according to size, internal structure, and motive. Their size varies from simple organisms to large transnational groups. Their organisational structure may be informal and lacking a chain of command, or formal and hierarchical with a differentiation of roles (often skills-based) and a structured system of command and control.[499] Some may be driven by political or ideological motives, while others act for financial gain.

Of the groups currently operating, Anonymous appears the most interesting, as well as the most challenging to match with the existing joint crime offences. As a matter of fact, the case of Anonymous is of pivotal empirical importance. The group has conducted a large number of attacks and has been addressed by a substantial amount of scientific analysis and case law. Small groups of hackers usually have a simplified structure, easily subsumed under traditional joint crime models. Conversely, Anonymous' enormous size, its transnational dimension, its strong ideological basis, its dynamism, and its permeability mean it has unique and significant operational and structural features.

The hacker collective Anonymous is commonly categorised as a hacktivist (a portmanteau of hacker and activist) group. In other words, it is an independent digital collective exclusively driven by political or ideological motivations. The very aim of Anonymous is to conduct acts of digital political-ideological protest.

The collective is undoubtedly the main actor in the political hacking panorama.[500] It exemplifies the stabilisation and internationalisation of the hacktivist phenomenon. Anonymous has existed since

---

[499] See, *inter alia*, T. J. Holt, 'The Attack Dynamics of Political and Religiously Motivated Hackers', in *Proceedings of the Cyber Infrastructure Protection Conference* (City University of New York 2009), 173: "For example, one site established its leadership and attack command structure based on individual performance in a hacking challenge set up through their website. Individuals must progress through 13 missions, and their performance establishes how they will participate in the larger group".

[500] See SurfWatch Labs, 'Anonymous Ops Trending, Where are The Other Hacktivists?' (SurfWatch, 26 May 2016) <https://blog.surfwatchlabs.com/2016/05/26/anonymous-ops-trending-government-targeted-where-are-the-other-hacktivists/>.

2003. Under its name, hundreds of ideologically-motivated attacks – from Denial of Service attacks[501] to information stealing – have been carried out.

In its complexity, Anonymous is both an international hacktivist collective, with members worldwide, and an umbrella network providing connections between hacktivists and subgroups. To consider it a "group" would be misleading, and the collective itself makes a point to highlight this fact. In a 2010 press release the collective stated: "Anonymous is not a group, but rather an Internet gathering".[502] It could be argued that the collective represents more of a "signature" for certain actions, an ideological umbrella and, most importantly, a structure under which sub-groups and individual hacktivists operate.

Anonymous has its origins in the "4Chan" forum, a still active image board website. [503] 4Chan users started with a series of non-political ("lulz")[504] attacks, such as raids against virtual online communities.[505] In 2006, they organised the first politically motivated action. They conducted a series of DoS attacks against the website of a white nationalist and negationist running a broadcast.[506] Since then, the movement has acquired a marked political/ideological *raison d'être.* Gradually, the digital structures used for planning such attacks moved away from 4Chan. As noted by Olson, the 4Chan discussion boards were inefficient for organising attacks, since new posts were

---

[501] A denial of service attack is a type of cyber attack aimed at making a digital machine or network resource unavailable, usually by saturating the system with external communication requests. A distributed denial of service (DDoS) attack is a type of DoS attack involving the use of multiple compromised systems — usually through a botnet — in conducting the attack.

[502] See 'Anon Ops, A Press Release' (10 December 2010) <http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf>.

[503] See www.4chan.org. This (still-existing) forum does not require registration: everyone can choose a username and posts can be uploaded anonymously. Thus, most of the authors of the posts appear as 'Anonymous': from this, came the future name of the hacker group. At its apex, the forum had 7 million monthly visitors from all over the world. Thus, the social life of the forum was intense, and created a sense of community between the members. The anonymity, the lack of registration and the absence of models or limitations on the content of posts offered a complete liberty of expression to the community – in particular, in the '/b/' board of discussion, dedicated to random topics. 4Chan remains one of the main hotbeds for Internet culture, and several Internet "memes" were created and developed there. (Merriam-Webster Dictionary Online: Meme: an idea, behaviour, style, or usage that spreads from person to person within a culture <http://www.merriam-webster.com/dictionary/meme>).

[504] According to Enciclopedia Dramatica, an online website dedicated to Internet underground culture, "lulz" is a corruption of "lol" (which stands for Laugh Out Loud), and has the meaning of "the act of entertaining oneself with the misfortune of others" (<https://encyclopediadramatica.se/Lulz>). See also G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous* (Verso 2014), Chapter 1: On Trolls, Tricksters and the Lulz. Interestingly, Coleman notices how the term is an argot, a specialized terminology used by a subcultural group, which serves to enact secrecy, erect social boundaries and "stabilizing a set of experiences by making them available for reflection.

[505] On the 12th of July 2006, 4Chan users joined the Habbo Hotel online community, all as black avatars with Afro hair and dressed in a black suit. They flooded the game, creating swastika formations and impeding the use of the pools of the online world, with no other purpose than having fun and creating confusion. See P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Little Brown & Company 2013), 49-50.

[506] See J. L. Beyer, *Expect Us: Online Communities and Political Mobilization* (OUP 2014), 35.

uploaded in real time and threads changed rapidly.[507] However, 4Chan was initially used as a recruiting tool, while the Internet Relay Chat (IRC)[508] became the main forum to discuss and organise the attacks.[509]

Today, the digital structure of the collective has moved towards an independent system of websites integrated via the use of the IRC platforms. Such platforms allow instant group communication through "channels" (i.e. discussion areas that can be created by any user of the chat service) or private messages. Several Anonymous-related accounts on the main social media (e.g. Twitter, Facebook and Youtube) are instead used for campaigning and promotions of the ideals and the specific operations of the collective.[510] The nature and the implications of these virtual tools of aggregation, interaction, and promotion are reflected in the structural permeability of Anonymous. These virtual spaces are easily accessible and open to any interested or curious, good or ill-intentioned, person. It follows that any "newcomer" can give his/her contribution to the collective. At first glance, the phenomenon can thus be described as a horizontal, open aggregation of individuals in a virtual space. The above-mentioned openness, and a distinct absence of hierarchy (at least, as it will be pointed out, to some extent) are distinctive characteristics of the movement.[511]

Hacktivism as a collective criminal phenomenon is an intersection between organised crime, political protest and terrorism. Anonymous, for instance, presents elements belonging to all three categories. It conducts forms of political protest, but quite often its means and methods are unlawful. It commits crimes against (digital) property in an attempt to achieve political or ideological objectives. To some extent, it presents an organised structure aimed at committing cybercrimes with a temporal continuity. Nonetheless, Anonymous also lacks some of the prominent elements of the above-mentioned criminal phenomena. Its acts hardly present a sufficient gravity (and lack the special intent) to be qualified as terrorism. Furthermore, it does not present the extemporaneous and chaotic form typical of a political demonstration.

At most, Anonymous could be described as a communicative network aimed at systematically organising political protest. This very element of "systematisation" distinguishes the activities of the group from ordinary protests, bringing them nearer to the concept of organised crime.

---

[507] See P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (n 505), 50.

[508] The Internet Relay Chat is an Internet text-based conferencing system. See P. L Witt, 'Internet Relay Chat', in H. Bidgoli (ed), *Handbook of Information Security, Key Concepts, Infrastructure, Standards, and Protocols* (John Wiley and Sons 2006), 87 ff.

[509] See P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (n 505), 51.

[510] See *Imperva's Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack* (Imperva 2012), 8.

[511] See, for instance, the (rectius: one of the) ideological manifesto of the movement: *Postulates: An Anonymous Manifesto* <http://anonnews.org/press/item/199>: "Anonymous is everyone. Anonymous is no one. Anonymous exists only as an idea. You also can be Anonymous. Becoming Anonymous is simple. Just take action".

Organised crime appears to be a more general and "neutral" phenomenon than terrorism and political protest, and usually lacks any qualitative consideration with regards to the type of predicate crime involved. It could be argued that organised crime seems to be the legal category under which Anonymous could be more easily subsumed. From the analysis of the case law related to Anonymous (further explored *infra*), it is notable that no members of the group have ever been charged with terrorism or rioting offences. Most frequently, criminal organisation offences have been applied.

Is this correspondence only apparent? Shall large hacker groups, such as Anonymous, be considered as organised crime, or do they lack important elements required to fit into this category?

Preliminary considerations: aim and operational features…

Before exploring the degree of "organisation" displayed by hacker groups (and in particular Anonymous), a series of preliminary considerations should be made. The first relates to the fact that some specific operational features provided for in traditional joint crime offences may be *ex ante* inapplicable to certain forms of online collective criminality.

In terms of aims driving the actions of criminal organisations, various cybercriminal consortia exploit digital media inspired only by ideological or political motives. For instance, Anonymous is characterised and held together by ideological and political motifs. It has never conducted any attack aimed at obtaining financial or material benefit. Many organised crime offences envisage a requirement of a financial aim of the group. In such a case, hacktivist groups such as Anonymous will be left outside the scope of the offence.

Furthermore, the operational features usually required by organised criminal offences appear not to fit the cases of Anonymous or hacktivism more broadly. Consider secrecy. Many hacker groups are hidden in cyberspace. Conversely, hacktivist groups openly advertise their operations on social media and websites. Notwithstanding the existence of private "invite only" channels within the Anonymous' IRC structure,[512] its discussion areas are open and accessible to all. Consider also the requirement of use of corruption, intimidation, or physical violence envisaged by organised crime offences. It appears to be inapplicable to any form of digital crime (unless, by stretched and questionable analogical interpretation, this requirement covers "digital" violence).

[512] See G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous* (n 504), 221, 222.

…and an important note on digital communication particularities.

The second preliminary consideration is related to the digital nature of online interaction. As discussed, communication is fundamental to coordination amongst the members of a group. Communication and social contacts in online spaces, however, present a different characteristic than in physical spaces. This difference is based on the use of computers as a medium between the actors. In order to explore the organisational particularities of Anonymous and the level of coordination reported by the group, it appears important to briefly consider the dynamics that characterise digital communication and the important implications of this for coordination.

A series of elements may reduce the effectiveness of online communication and negatively impact the quality of online group coordination. From a subjective point of view, a cyber user may contemplate his/her possible online actions and their implications with a greater degree of detachment than an actor operating in the physical world. Especially within an online group, this may influence its social behaviours.

John Suler, in his landmark work on the "online disinhibition effect", identifies six elements that induce depersonalisation of the actors and their dissociation with their online actions. These are: the dissociation between one's online and offline identity, and the ability to keep the latter identity hidden – "dissociative anonymity" or "you don't know me"; the awareness of being physically invisible to the other – "invisibility" or "you can't see me"; the lack of real time reactions and interaction – "asynchronicity" or "see you later"; the creation of imaginary characters and/or features of other users, given the absence of physical information about them – "solipsistic introjection" or "it's all in my head"; the dissociation of what is perceived as online fiction as opposed to offline facts – "dissociative imagination" or "it's just a game"; and the lack of expression and perception of the status and power of other users, which may influence command and control dynamics – "minimisation of authority" or "we are all equals".[513]

Furthermore, the lack of proximity and physicality in computer-mediated interaction reduces communicative sensations. Communicative interaction is not exclusively based on the significance of the message. Conversely, it relies heavily on metalinguistic addenda, which are primarily conveyed by sound (intonation) and body language. Such addenda are completely lacking in computer-mediated communication.[514] Any posts or online texts may thus be subject to a certain degree of

---

[513] See J. Suler, 'The online disinhibition effect' (2004) 7 Cyberpsychology & Behavior 321. See also: "John Suler's The Psychology of Cyberspace" <http://users.rider.edu/~suler/psycyber/disinhibit.html>.

[514] Notwithstanding the use of graphic signs, such as emotion icons (emoticons), in order to convey metalinguistic meaning. See E. Dresner and S. C. Herring, 'Functions of the nonverbal in CMC: Emoticons and illocutionary force', (2010) 20 Communication theory 249.

misunderstanding. A facetious message can be interpreted as sincere, and *vice versa*. A lack of communicative sensation may then reduce the "regulatory feedback" in online conversations and could trigger spiralling misunderstandings. This lack of adequate understanding reduces the coordination of communication,[515] thus decreasing the quality of social interaction. From a behavioural point of view, online interaction appears less cohesive and coordinated than its physical equivalent.[516] Such considerations should be taken into account in any analysis of online-based criminal groups, and their organisational structure.

Communication.

As previously mentioned, Anonymous expresses its social life exclusively online, on a series of independent websites, IRC chat platforms and social media. The latter are used for campaigning and for promoting the ideology and the specific operations of the group. These fora are also used for attracting attention, endorsement and support of the group's cyberattacks.[517] Core discussions and deliberations are conducted on IRC servers, both on the open web (e.g. "Anonymous Operations") and on the so-called deep web (e.g. Onion IRC).[518]

Two levels need be identified within these discussions. The "general level" of discussion includes conversations and interactions related to subjects linked to the ideological position of the group as a whole. The "operational level" is used for more specific discussions related to specific areas of possible actions.

---

[515] See S. Kiesler, J. Siegel and T. W. McGuire, 'Social Psychological Aspects of Computer-Mediated Communication', (1984) 39 American psychologist 1123, at 1125. See also R. E. Kraut, S. H. Lewis and L. W. Swezey, 'Listener responsiveness and the coordination of conversation' (1982) 43 Journal of personality and social psychology 718.

[516] On the other hand, from a *mens rea* perspective, an online criminal agreement – or, more in general, any purposive criminal discussion or proposal on the web – requires less psychological effort. To some extent, if culpability is focused on the state of mind of the actor, it may even be argued that the digital character of the act mitigates its blame, at least in the sense of a reduced awareness of the consequences of their action and the appreciation of its moral wrongfulness. In reference to a concrete example, even if we consider the use of Facebook to incite to street disorders as endangering public security and eventually deserving punishment, we are usually prone to recognise here a different culpability than in physically inciting to riot a group of protesters (see H. Carter, 'England riots: pair jailed for four years for using Facebook to incite disorder' (The Guardian, 16 August 2011) <https://www.theguardian.com/uk/2011/aug/16/uk-riots-four-years-disorder-facebook>).

[517] See *Imperva's Hacker Intelligence Summary Report* (n 510), 8.

[518] See "Anonymous Presents: The Onion IRC" <http://www.anonymousvideo.eu/anonymous-presents-the-onion-irc.html>. Onion routing is a technique used for hiding the origin of a packet of data. Originally patented by the U.S. Navy, the technique involves a series of routers through which the packet is sent. Every intermediary router accepts the encrypted package without knowing its content, its origin or destination. It re-routes it towards another randomly chosen node. The first router adds a number of encryption layers to the packet: through this process, every router "peels" a layer of encryption. In this manner, the file appears different in every router and cannot be tracked. TOR (The Onion Routing) is open-source software that enables online anonymity through onion routing.

The first level of discussion is held in general public channels, specifically created for that purpose. Some of these channels are international, others host discussions of the national subgroups of Anonymous.[519] Operational discussions and deliberations are instead hosted in distinct sections of the group's communication channels.[520] These sections can be generated collectively by a group of users, or autonomously created by individuals.

Interestingly, the operational channels do not contain specific instructions, indication of targets and provision of tools[521] to be used to carry out cyberattacks. Such information, which is necessary to ensure basic coordination of the group during the operational phase, is usually found on linked "pastebin" websites pages (such as "Pastebin" or "Ghostbin")[522]. As a matter of fact, such websites offer the possibility of storing plain text that otherwise could be easily lost in a chat room, where real-time communication constantly flows. Some of these pages contain static, unmodifiable text, and are created by one or few hackers. Others (although very few) can be integrated and modified by users, and thus reflect a true model of collective deliberation.

Organisational structure.

At first glance, it seems difficult to identify an organisational structure through which Anonymous plans, coordinates and conducts attacks. The group has no vertical hierarchy or pyramidal structure, from which a chain of command and control propagates. There is no central entity that controls the overall network or allocates roles and tasks.

Furthermore, the organisational features of the group do not indicate the existence of a horizontal structure. No structural linkage connects the channels of discussion to the operational channels. All channels are openly joined and left by members "surfing" the network.

This appears to be in line with the way Anonymous describes itself as a "leaderless" collective. However, the complete absence of a hierarchical structure is easily debunked by a less superficial

---

[519] See, e.g., S. K. Bertram, 'Authority and Hierarchy within Anonymous Internet Relay Chat Networks', (2015) 6Journal of Terrorism Research 1, 27ff.

[520] For instance, "#OpIsis" was the channel related to the operations against the terrorist group Daesh.

[521] Interestingly, the indication of the so-called "tools" of attack does not take the form of a concrete provision of instruments for the material conduction of the attacks. It usually encompasses a simple indication of programs provided by third parties, which may be accompanied by statements on limitation of liability in case of their use for the commission of offences.

[522] The movement gradually passed from Pastebin to Ghostbin, a website created by Anonymous itself, due to Pastebin's struggle to remove "sensitive information" posted to the site by hackers (see E. Protalinski, 'Pastebin to hunt for hacker pastes, Anonymous cries censorship' (Zero Days, 4 April 2012) <http://www.zdnet.com/article/pastebin-to-hunt-for-hacker-pastes-anonymous-cries-censorship/>; Meet Hackers Editorial Team, "Ghostbin a New Form of Pastebin" (MeetHackers.com, 16 May 2014) <http://www.meethackers.com/2014/05/ghostbin-new-form-of.html>.

analysis of its social mechanisms. Studies on the hacktivist collective[523] highlight the existence of a loose hierarchical structure. As a matter of fact, IRC channels envisage an administrative distinction between "operators" and ordinary users. To ensure a minimum level of moderation and control of the channels, a special class of privileged users, i.e. "operators", (originally the creators of the channel, who may eventually appoint other users), are equipped with a series of powers: to perform general maintenance functions, such as disconnecting and reconnecting servers; to terminate the channel; and, most importantly, to remove a user from the channel in order to avoid any abusive behaviour (such as repeatedly sending the same message, thus saturating the channel).[524]

The existence of such privileges, and the effect of their use, was studied in a notable work by Stewart Bertram.[525] Bertram's study includes a quantitative analysis of the relationship between privileged and ordinary users within a single channel and within the whole network of Anonymous. Furthermore, the work conducts a comparative analysis of two channels: an operational channel named "#OpGreenRight" and a general discussion channel of the Australian community. The analysis reports different relationships between privileged and ordinary users in the two channels. In the former, besides having the ordinary power of removing those users that were not in compliance with the implicit rules of the community, the operators were only given the role of providing suggestions to the other users. Such suggestions, however, were nor enforced, nor necessarily complied with.[526] In the latter channel, *per contra*, also due to the smaller numbers of participating members, it was possible to find, according to Bertrand, a "strong system of hierarchy" and an "overt social control"[527] carried out by a stable subgroup of (five) operators which, albeit receiving constant challenges, "initiated and closed most conversations, enforced cultural norms and generally set the tone and pace of any cyber activity" in which the group engaged.[528]

It is contested, however, whether the "strong system of hierarchy" described by Bertrand amounts to a system of coordination or of command and control. The authority of an administrator is likely to derive from his/her thorough knowledge of the aims and functioning of the collective, or to be related to his/her technical skills. However, most of all, it can be rooted in his/her "online charisma".[529] Administrators do not possess any instrument of command or control apart from their

---

[523] See in particular, P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (n 505); and S. K. Bertram, 'Authority and Hierarchy within Anonymous Internet Relay Chat Networks' (n 519).

[524] See J. Oikarinen and D. Reed, *Request for Comments n. 1459. Internet Relay Chat Protocol* (May 1993).

[525] See S. K. Bertram, 'Authority and Hierarchy within Anonymous Internet Relay Chat Networks' (n 519).

[526] *Id.,* 27.

[527] *Ibidem.*

[528] *Id.*, 28.

[529] Although channels can be "taken over" by other hackers, forcing all legitimate users out of a channel – for instance, through a Denial of Service attack – thus obtain the privileges.

limited administrative tools. Hence, their influence and ability to coordinate other members derive from their prestige.

The relationship between administrators and ordinary members is better described in terms of influence than domination or command or control.[530] Furthermore, the power of administrators usually does not extend outside of the channel in question. Nor does it control the operative and conduction phase, which is carried out by individual members.[531] The outcomes of this administrative distinction thus appear to be limited to social and behavioural influence.

Aside from normative vertical structures based on an institutionalised system of roles, hierarchy may originate from social or behavioural norms active within a group.[532] As the protagonist of Pessoa's "The Anarchist Banker" decries, even where there is a formal rejection of social roles of dominance and subordination, members of a group with sufficient stable interactions are prone to spontaneous self-regulation. They modulate their interactions via psychological unconscious behaviours. Thus, hierarchical ranks (although not based on status and authority) are concretely generated. This type of hierarchy is highly susceptible to variation and displays a lower level of stability and demarcation of roles. Within it, the division of roles is not allocated *ex ante,* according to a stable system. Rather, it is distributed amongst members on the basis of an unconscious social process. Nonetheless, it still is a *de facto* hierarchy.

Such behavioural influence and *de facto* hierarchy undoubtedly exist within Anonymous. The extent and rate of behavioural influence, and the type of hierarchy that results from it, differs according to the nature of interactions. The more a group stabilises, the more each participant will find an implicit role in the societal warp, whether institutionalised in the administrative status or not. They create emotional bonds to the others that may lead to mimesis. In stable and continuous channels

---

530 See M. Diani, 'Leaders or brokers? Positions and influence in Social Movement Networks', in M. Diani and D. McAdam, *Social movements and networks: Relational approaches to collective action* (OUP 2003), 106.

531 A real position of control over the behaviour of the members of the collective, if any, could be found in the creation stage of the operative phase and of the pastebins containing instruction and targets of the attacks. Yet, also here, the relationship of control is indirect. The indications, even if they are likely to be followed by the members participating in an attack, are still lacking any coercive enforceability. It should be finally noted that within the Anonymous network, there are areas where only some members (operators? most known hackers? most technically-skilled? hacker subgroups?) are allowed to enter: private "invite only" channels. See G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous* (n 504), 221-222. It can be likely affirmed that some of the decisions on the operations are taken here. Interestingly, on the news platform of the collective, AnonNews, an alleged 'former member' of AnonOps (the Anonymous' IRC) affirmed: "From the fucking beginning (during the hack at Aiplex which started Operation Payback) there has been a secret club, an aristocracy in AnonOps, deciding how operations will play out in invite-only channels. It's obvious, for they control the topic, the hivemind, the guides, every single thing behind the scenes. (Sic)." The message was posted on AnonNews on 8, May 2011 and was accessible untill May 2014 at <http://www.anonnews.org/?p=comments&c=ext&i=1571>. However, currently, AnonNews.org appears to be unavailable.

532 See e.g. T. Diefenbach and J. A. Sillince, 'Formal and informal hierarchy in different types of organization', (2011) 32 Organization Studies 1515.

with low mobility, the amount of interaction within the same group may induce the emergence of charismatic leaders, together with a set of behavioural norms followed by the participants. Yet, even in ephemeral areas – such as in the operative channels of Anonymous – there can be moment of discussions on the proposed actions. As pointed out by behavioural scholars, in these fora, certain individuals can be more charismatic and prominent than others. These actors are likely to define and propose actions that will be widely endorsed by the other participants. [533] Thanks to the interaction between individuals, and the leading behaviour of "keynoters", a certain spontaneous social organisation may thus emerge even in such ephemeral spaces.

However, the extent of these sociological considerations should be understood in light of the scientific findings mentioned above. According to classical and computer-related theories of group behaviour, a lack of physical interaction, coupled with the element of anonymity, tends to decrease the identification, surveillance, control, and accountability of members, as these factors are related to the intensity of the social contact, mutual social influence, and general conformity with the group.[534] Therefore, the social morphology of an online group, and its internal system of relationships, are likely to be less organised than those of a group operating in physical reality.

This theory may be applicable to the ephemeral reality of the social structure of Anonymous, producing diminishing effects on the authority of the administrator, on the mutual influence between its members, and on the influence of charismatic members. Nonetheless, the "solipsistic introjection" phenomenon – i.e. the creation of imaginary characters and features for others in the lack of physical information about them – may work as a magnifier of charisma and influencer of keynoters, up to and including the creation of leaders expected to lead the "fight for freedom".

Considering all the above, it may be concluded that *Anonymous* does not present the features of a homogeneous entity and is not hierarchical *per se*. Approaching the study of this hacktivist phenomenon through a sociological lens allows a better understanding of its decentralisation. Under the umbrella of this intriguing organisation, it is possible to find, on the one hand, dynamic processes composed of a high number of lone participants, who surf the channels freely and, absent a properly system of enforceable command and control, autonomously decide upon the extent of

---

533 See e.g. R. H. Turner and L. M. Killian, *Collective Behavior* (Prentice Hall 1959).

534 See M. Deutsch and H. B. Gerard, 'A study of normative and informational social influences upon individual judgment' (1955) 51 The journal of abnormal and social psychology 629, 629; S. Kiesler, J. Siegel and T. W. McGuire, 'Social Psychological Aspects of Computer-Mediated Communication' (n 515), 1125; T. Postmes, R. Spears, K. Sakhel and D. De Groot, 'Social influence in computer-mediated communication: The effects of anonymity on group behavior' (2001) 27 Personality and Social Psychology Bulletin 1243, 1244. Furthermore, in the absence of a set of unifying factors based on visualisation and spatial-temporal unity within the members, the imitative phenomenon that is composed of reciprocal suggestion, imitation, and contagion – i.e. the cornerstone of the classic "pathological" theory of criminal crowd behaviour theorised by Sighele and Le Bon – loses most of its importance.

their participation in the discussion and operative phase. On the other hand, the crystallisation of more structured areas, such as channels wherein there is a more static presence of a set subgroup of members, and where a stronger hierarchical system has been spontaneously generated, is notable. Most commonly, subgroups formed through this latter process show a higher degree of independence from the collective and may eventually evolve into independent groups, or at least even be perceived as such by those directly involved.

Coordination within the nodes.

A certain level of coordination may exist within collectives such as Anonymous. This coordination can be based on behavioural hierarchies between members, or be supported by the relevant administrative powers of privileged users, or both. However, no structural coordination is found between the various areas or channels of the collective. No common plan is conceived by the group as a whole and followed by the decentralised nodes. This is due to the lack of centralised deliberation or of a superior central leadership directing or facilitating coordination within the various channels. An operation can be decided, launched, and carried out by a small group of users, without any cooperation or approval by the rest of the collective.

What really provides a basic operative coordination within the collective appears to be a set of ideological beliefs and ethical standards shared by the members. Indeed, hacktivism is the expression of a precise subculture, with specific moral and ethical standards. These standards derive both from the classic hacker ethics[535] and from general principles linked to the protection of

---

[535] See e.g. S. Levy, *Hackers: Heroes of the computer revolution* (Penguin Books,2001). See also the Final Declaration of the International Conference on the Alternative Use of Computer" (also called "Galactic Hacker Party") held in Amsterdam in 1989: 'The free and unfettered flow of information is an essential part of our fundamental liberties and shall be upheld in all circumstances. Information technology shall be open to all, no political, economic, or technical consideration shall be allowed to impede this right. Government shall be fully accessible to all people at all time. Information technology shall enhance the scope of this right, and not reduce it. Information belongs to the people and is made by the people. Computer scientists and developers are in the service of the people and shall not be allowed to develop into a caste of privileged and unaccountable technocrats. (…) Computer technology shall not be used by governments and corporate bodies to control and oppress the people, but shall on the contrary be used as an instrument of emancipation, advancement, learning and leisure. Likewise, computer technology, and science in general, shall be removed from the hands of the military establishments. (…) Computers and information technology shall become a tool to revolutionise our living planet." (International Conference on the Alternative Use of Computer, *Final Declaration*, <https://n-1.cc/bookmarks/view/1663318/galactic-hacker-party-and-icata89-in-amsterdam>).

fundamental human rights.[536] The ideological hummus works as an engine for members' contribution to the group, as an external limit to their actions, and as an operative connection between the various areas of the group.

An instance of this is the fact that social media accounts are not created and managed by an established set of users. From a strictly structural point of view, the managers of accounts all act independently. Their factual operative homogeneity relies on the set of shared ideological beliefs and ethical standards guiding the actions of the organisers. Similarly, throughout the discussion phase, the proposed ideological contribution of users is discussed and accepted only if consonant with such principles. Furthermore, the various operational areas are also held together by their correspondence with the ethical principles of the subcultures from which Anonymous stems. Their reception by the collective, the extent of participation they attract, and their final success are ultimately based on their assonance and relevance in relation to these principles. All the actions that lie outside of such ideological compliance will not be followed and, eventually, will be strongly rejected by the community.

In conclusion, it can be asserted that the various areas within Anonymous are primarily linked by the shared ideological and ethical beliefs shared by its members. However, there is no trace of any structural and *ex ante* established mechanism of coordination, neither between its members, nor throughout the various phases of its online activities or between the various channels of communication therein. Therefore, the lack of coordination between the nodes should exclude any unitary consideration of Anonymous as a superstructure, least of all in terms of liability purposes.

---

[536] See, inter alia, "Anon-combat-index: What is Anonymous?" <https://ghostbin.com/paste/tfgst> "Anoynmous is not a group, it is not a person. It is an idea. Specifically it is the idea, that all of us deserve FREEDOM. Freedom of thought, of speech, of expression, of knowledge, of belief. The Freedom to determine the course and destination of our own lifes. If your share this IDEA, THAN YOU ARE ANONYMOUS. You have likely heard many things about Anonymous, some of them are true and some of them are not. We are not hackers. We are not terrorists. We are not violent. We are citizens of the world who bear witness to tyranny, oppression and censorship. We are activists who seek to change the system and the cycle of corruption. We seek to create transparency in governments and all institutions of public service. We resist those who seek to violate our rights as human beings. As a collective of autonomous individuals however, WE HAVE NO LEADERS who dictate the methods of resistance. Some of us are indeed hackers, who use our skills to make critical information available to the public. Some of us organize protests and rallies. Some of us volunteer our time to feed those who can't feed themselves. We are your neighbours, your friends, and your relatives. We prepare your food, repair your appliances, write your books, compose your music, and create your technology. We are your postal workers, barbers, store clerks and lawyers. We are socialists, capitalists, we are atheists and we are religious, WE ARE EVERYONE and we are no one. NONE OF US ARE AS POWERFUL AS ALL OF US. United as One, Divided by Zero. WE ARE ANONYMOUS."

Cohesion.

As previously pointed out, another pivotal element that defines a criminal organisation is its internal cohesion, and the solidity of the bounds between the individual and the group. In Anonymous, there is no system of initial admission and acceptance of group members. Anyone can extemporaneously enter the network and participate in the social life of the group. A kind of behavioural unity is afforded by the set of non-written cultural-ethical norms that is shared by the collective. Such norms work as an external limit to the participation of new members. The community will not accept the behaviour of a member that conflicts with the core ideology of the group.[537] However, individual commitment to a shared set of ethical rules or ideological beliefs can hardly ensure a stable cohesion of the group.

What about accountability? As previously noted, *Anonymous* possesses a rudimentary system of sanctions. However, the authority of privileged users does not become a system of command and control amongst members. In particular, any command and control of an individual's actions is missing during the operative phase. Here, every contribution to the attack is provided autonomously and separately. Furthermore, from an empirical analysis, the system of internal sanctions is usually limited to gross violations of explicit and implicit ethical group norms. In a collective that perceives itself as leaderless, any excessive use of such power will likely be considered as contravening a fundamental ethical norm of the group, and thus lose its legitimacy.

Nonetheless, as demonstrated by Bertram's analysis of Anonymous, the stability of a subgroup increases the importance of authority. The more stable subgroups become, the less influential the psychological/sociological factor of "dissociative anonymity" results will be. In stable interactions, the dissociation between the online and offline identity of users is likely to decrease. Conversely, the level of attachment felt towards the group usually increases. Members of subgroups are, therefore,

---

[537] A set of written rules regarding the use of the common spaces does exist. Interestingly, none of these rules expresses a system of command and control, nor relates to criminal incitement or purpose. On the contrary, these rules explicitly ban certain criminal behaviours, such as pedopornography or carding frauds. In case of AnonOps, these rules are:
"1) When requested, please use English in channel. We have international channels. We realize you may speak another language, respect that we do, too. 2) If you're an asshole, we will treat you like one. 3) Don't spam or flood the channels, use of ascii art is spam. If you want to paste a link to your personal site, twitter, or channel ask first. Please do not advertise other IRC networks here. 4) User bots or scripts with public triggers are not allowed unless authorized by staff, and are following the rules stated in #bots. 5) No multiple connections from your location. As a user you only need 1 connection. Exceptions can be made for valid reasons such as bouncers, VPNs. Join #help and speak to an IRCop. 6) Child pornography is expressly FORBIDDEN everywhere. See https://anonops.com/aup.html for more information. 7) Carding in any form is FORBIDDEN everywhere. 8) Do not impersonate another user or use oper nicks in your own. 9) We are not a marketplace, do not try to advertise, sell your botnet, or other services here. 10) Do not use URL shortening services, paste the full URL. 11) IP harvesting in any form is not allowed, we cloak user IPs for a reason. 12) We do NOT allow any user to connect any type of ddos/flood/spam bots to this network. 13) Do not ask for personal information from other users." See: '#AnonOps Channel Rules' < http://anonops.com/chanrules.html>.

likely to feel more accountable for their actions, and be held to that standard. As a consequence, members of subgroups may become more prone to act according to the behavioural norms of the group. With a stable participation in an IRC channel, the members will likely gain a social status within the subgroup. They may grow fond of and want to defend that status, lending greater significance to the ostracising power of administrators. Furthermore, despite the fact that a certain level of offline anonymity will continue to be enjoyed by members, their visual anonymity (Suler's "invisibility") may also tend to lessen the importance of personal features and interpersonal differences, while favouring a focus on the social identity of the group and its characteristics.[538] It thus seems reasonable to suppose that all of these factors strengthen the overall level of cohesion within a subgroup.

Stability and self-perpetration.

Another element usually considered to define organised criminal groups is their stability. The Anonymous' structure has existed since 2003, and, under its auspices, hundreds of attacks have been carried out. However, as seen so far, this structure is heavily decentralised.

While the structural exoskeleton is stable, its living nodes show a high degree of evanescence. Amongst the channels of the collective, only the core structure seems to express any form of stability. Many of the general channels have existed since the very creation of the Anonymous' IRC Servers. However, these channels are limited to general and licit discussions, and are not stably linked to the operative parts of the IRC structure. The operative channels, instead, are closed at the conclusion of operations. However, it should be noted that a single operation may encompass various criminal episodes, with different types of attacks perpetrated in the course of a few days. Whether such an operation meets the temporal stability criterion depends, therefore, on the modulation of the requirement in the relevant legal system.

The stability of the group, as mentioned, crucially includes its continuity, or self-perpetration. This requirement is fully met by Anonymous. Due to its amorphous features, substantial lack of formal hierarchical structure, and high permeability, even if members quit or are arrested the entity continues to exist.

---

[538] See T. Postmes, R. Spears, K. Sakhel and D. De Groot, 'Social influence in computer-mediated communication: The effects of anonymity on group behavior' (n 534), 1224.

II.VII.X.TESTING THE PAIRING: DOMESTIC CASE LAW.

By testing the lens used in the criminological and legal definitions of organised crime, the analysis of *Anonymous* that has been conducted so far has exposed some unique features of the phenomenon. The question has to be asked as to how national judiciary systems have taken these peculiarities into account. The following section will investigate some of the most interesting examples of application of joint crime offences to the hacktivist collective.

Over the past years, the number and the scale of attacks conducted by the group has increased. The collective has received broad media coverage, and several charges have been brought against Anonymous. In many cases, members of the collective have been charged with specific cybercrime offences, as well as with joint crime offences. As will emerge from the following review of existing case law, various legal solutions have been used to prosecute the criminal manifestations of Anonymous as collective crimes. The difference, however, does not rely exclusively on the nuances of the joint crime models applied. Due to the original character of the work conducted in such operation (subsuming a new criminal phenomenon under a traditional model) the final judgments have been most likely influenced by the degree of understanding that the trial actors had of Anonymous and its functioning. Therefore, the level of accuracy of the investigations carried out by the relevant authorities and of the resulting criminological depictions of Anonymous as a structure are likely to have played an important role in orienting the judgments of the courts.

Common law systems.

Up until today, common law systems have never applied structured models of criminal association – such as the RICO offence or the new UK criminal association offence – on hacker groups. In 2013, the RICO was used by the District Court of Nevada on the cyber organisation "Carder.su", which bought and sold stolen personal and financial information through online fora.[539] However, this

---

[539] See US, *United States of America v. David Ray Camez*, No. 2:12-cr-00004-APG-GWF (2014); J. W. Salvador, 'Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime' (2015) 41 Rutgers Computer & Technology Law Journal 268; US, District of Nevada, Attorney's Office, Press Release, 'Man Who Bought and Sold Stolen Personal Information Online Convicted of Participating in Racketeering Organization' (6 December 2013) <https://www.justice.gov/usao-nv/pr/man-who-bought-and-sold-stolen-personal-information-online-convicted-participating>; US, Department of Justice, Office of Public Affairs, Press Release, 'Member of Organization That Operated Online Marketplace for Stolen Personal Information Sentenced to 20 Years in Prison' (15 May 2014) <https://www.justice.gov/opa/pr/member-organization-operated-online-marketplace-stolen-personal-information-sentenced-20>; M. J. Schwartz, 'Cybercrime Milestone: Guilty Verdict in RICO Case', (Informationweek, 12 December 2013) <http://www.darkreading.com/attacks- and-breaches/cybercrime-milestone-guilty-verdict-in-rico-case/d/d-id/l 113050>.

organisation had structural features that were completely different from those of Anonymous. They perfectly matched the ascribed model of organised crime. First, the organisation was highly structured with diversified roles and ranks. Second, it had a fixed membership and a strong level of internal cohesion and stability. Finally, it employed a strict system of group approval for new members. [540]

With regards to Anonymous, several members of the collective have been charged on counts of criminal conspiracy.[541] As mentioned in the first section of the subchapter, the concept of conspiracy is centred on the agreement between the co-conspirators and lacks the "hard" structural requirement of most civil law criminal organisation offences. In relation to these cases, therefore, it seems superfluous to analyse how the overall organisational features of the group were subsumed under the legal concept of conspiracy. It is rather preferable to focus the analysis on the extent of the contested conspiracy agreement.

In a case related to the infamous Steubenville rape, a member of Anonymous was accused of having "together with others, knowingly and intentionally joined and voluntarily participated in a conspiracy and agreement to commit offenses against the United States".[542] Interestingly, the extent of the criminal agreement contested is very precise and was not stretched to apply to the rest of the network. In this case, the judge did not consider *Anonymous* in its whole structure and restricted the argument to the proven facts related to the online agreement between the individual conspirators. The case focused on a specific agreement between two members of the collective, manifested in

---

[540] US, Department of Justice, Office of Public Affairs, Press Release, 'Member of Organization That Operated Online Marketplace for Stolen Personal Information Sentenced to 20 Years in Prison' (n 539). According to the Attorney's Office: "The organization operated an internet web portal called a forum, where members could purchase the illicitly obtained data and share knowledge of various fraud schemes. A second forum was also created to vet incoming new members. The forums were generally hosted within the former Soviet Union and the upper echelon of the organization resides within the former Soviet Union. It was estimated that in July 2011, there were over 5,500 members of the organization. It was determined that members of the organization had different roles, including moderators who directed other members in carrying out activities; reviewers who examined and tested products, services, and contraband; vendors who advertised and sold products, services and contraband; and members. Members were required to successfully complete a number of security features designed to protect the organization from infiltration by law enforcement or members of rival criminal organizations."

[541] See, *inter alia*, US, *United States of America v. Collins*, et al., 13 CR 383 (2013); US, *United States of America v. Cooper, et al.*, 11 CR 471 (2013); US, *United States of America v. Lostutter*, 5:16-cr-00062 (2016). UK (England), *R v Christopher Weatherhead, Ashley Rhodes, Peter Gibson, and Jake Burchall*, unreported, Southwark Crown Court, (24 January 2013).

[542] US, *United States of America v. Lostutter* (n 541): …"that is, intentionally and without authorisation accessing a computer used in or affecting interstate or foreign commerce or communication, and thereby obtaining information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the states of Ohio and Kentucky, specifically invasion of privacy, libel, Ohio Revised Code §§ 2909.07(A)(6)(a), 2913.04(B), and Kentucky Revised Statutes §§ 434.853, 526.050, 526.060. All in violation of 18 U.S.C. § 1030(a)(2)(C) and 18 U.S.C. § 1030(c)(2)(B)(ii)." Interestingly, the aim of the conspiracy was, according to the indictment, to "gain publicity for their online identities".

various privately shared messages. Although the conspirators largely acted within the structure of Anonymous, the indictment did not mention the collective.[543]

Per contra, in an important case related to a series of attacks conducted within the framework of one of the biggest Anonymous' operations, "Operation Payback",[544] the extent of the conspiracy considered by the court covered the whole operation and a relevant part of the structure of the collective. Thirteen members of Anonymous were charged in the Eastern District of Virginia, US, with the crime of conspiracy to intentionally commit damage to a protected computer. It is interesting to note that the indictment describes the whole operational phase, in its planning, recruiting and participating steps. According to the indictment: "OPERATION PAYBACK targeted victims worldwide, including governmental entities, trade associations, individuals, law firms, and financial institutions, which ANONYMOUS claimed opposed its stated philosophy of making all information free for all, including information protected by copyright laws or national security considerations. As a result, the defendants, together with other ANONYMOUS members known and unknown to the Grand Jury, launched, or attempted to launch, cyber-attacks against entities including the Recording Industry Association of America ("RIAA") in the Eastern District of Virginia, the Motion Picture Association of America ("MPAA"), the United States Copyright Office of the Library of Congress, Visa, MasterCard, and Bank of America, and caused significant damage to victims."

Specifically, the defendants are accused of having: "participated in a worldwide conspiracy as part of the online group ANONYMOUS (…) to engage in a coordinated series of cyber-attacks", and "knowingly and intentionally conspired and agreed together and with each other, and with others known and unknown to the Grand Jury, including unindicted co-conspirators known and unknown to the Grand Jury, to commit an offense against the United States [a coordinated series of cyber-attacks against victim websites]".

Furthermore, it is specified that the accused: "used and, in some cases, publicized and distributed to other ANONYMOUS members (…) a freely-available and downloadable network stress testing program known as the Low Orbit Ion Cannon ("LOIC")" to conduct DDoS attacks" and "participated in and coordinated these DDoS cyber-attacks − deciding on the next target; publicizing the victim names and IP addresses; announcing dates, times, and relevant instructions; downloading the LOIC tool; and recruiting more attackers − through postings (collectively, "fliers")

---

543 See e.g. D. Kushner, "Anonymous v. Steubenville" (Rolling Stone, 27 November 2013), <http://www.rollingstone.com/culture/news/anonymous-vs-steubenville-20131127>.

544 Operation Payback begun primarily in retaliation to the discontinuation of "The Pirate Bay," a Sweden-based file-sharing website dedicated to the illegal downloading of copyrighted material.

on web bulletin boards and through social media and dedicated online chatrooms known as Internet Relay Chat ("IRC") channels." [545]

However, the positions and roles of the specific defendants were not necessarily central within the overall structure of the collective. Nor did they seem to have had any core participation in the organisation of the attack. The indictment took into account all the attacks conducted within the framework of the operation. Nonetheless, these are considered to have been committed in furtherance of a unique conspiracy.

Furthermore, in several of the aforementioned attacks, the defendants had no participation, with those attacks being generically attributed to "members of the conspiracy" (i.e. other users of the IRC channels). The indictment did not attempt any classification according to ranks, but merely specified that one defendant had the position of channel operator. Nor did it satisfyingly clarify the role of the defendants in the conspiracy.

The indictment solely mentioned that some of the defendants had (or attempted to have) some influence within the channel as some had offered to "edit a propaganda flier announcing the attack"; explained how to use the LOIC tool; posted menacing messages on the channels against the targeted entities; indicated targets; or incited other members to carry out the attack. Other defendants, instead, had merely participated in the attack by using the LOIC tool.

Moreover, in this case, the structure of Anonymous retained a pivotal position, as it is implicitly considered to be the link between the conspirators, i.e. the organisational element that materially kept them together under a larger conspiracy agreement. The network, nonetheless, does not receive sufficient attention to justify such consideration. As an example, mere use of the LOIC tool – which is autonomously downloadable and utilisable through indications found in the platform – to conduct an attack, does not necessarily entail being part of a criminal agreement or interacting with other members. However, according to the indictment such use amounted to a participation "in the DDoS cyber-attack on MasterCard, in concert with their co-conspirators".

From a legal point of view, factual proofs are more indicative of the existence and the functioning of an online criminal agreement, than the mere participation in the online social life of *Anonymous*. The latter approach to online criminal interaction should be avoided, especially where a precise analysis of the functioning of the network, backed by evidence, is lacking.

---

[545] US, *United States of America v. Collins*, et al. (n 541).

Civil law systems.

As largely evidenced in the previous chapters, in comparison with conspiracy, the criminal association models are more focused on the structural elements of the organisation. Their application thus requires a deeper analysis of the sociological and criminological traits of the group. A few interesting cases have been brought against members of Anonymous under participatory-type joint crime offences, in particular in Europe.

In France, in relation to a series of cyberattacks against public and private websites, three alleged members of Anonymous were charged on various counts with cybercrimes and with the aggravating circumstance of committing the offences within the framework of a *bande organisée*, provided for in Art. 323-4-1 of the French Criminal Code. According to the indictment, the defendants participated in an operation – *Operation Grands Projects Inutiles et Imposés* – and had an active part in the planning and conduction of the related cyberattacks.[546] However, in the judgment of the Tribunal de Grande Instance de Nancy, delivered in late 2015, there was no specific analysis of the structure and organisation of the overall collective. The judges recognised the existence of an "executive council" within the operative channel. Unfortunately, they did not provide any further analysis of the issue. Interestingly, however, they chose to apply the broader concept of *association de malfaiteurs*, finding the narrower concept of *bande organisée* inapplicable in the case at hand. According to the Tribunal: *"les actes préparatoires à la commission de ces infractions comme notamment l'utilisation de moyens informatiques destines à announcer, susciter l'adhésion et la participation active d'autres internautes à ces attaques, l'utilisation des moyens nécessaires à tender anonymes les participants comme à revendiquer la réussite de ces attaques, sont constitutifs de l'élément materiel de l'infraction de participation à un groupment formée ou une entente établie en vue de la préparation des infractions précédemment évoquées et ne caractérisent pas la circonstance aggravante de bande organisée."*[547]

Notwithstanding the scarce analysis provided by this sentence, which does not shed light on the concrete applicability of the French joint crime offences to the case of Anonymous, the judges recognised the lack of a sufficient "structured organisation" to satisfy the requirements of a *bande organisée.*

---

[546] FR, Tribunal de Grande Instance de Nancy, *26JIRS/2015, 14357000066* (23 November 2015). One of the defendant, which was found as not having a direct participation in the attacks, have been acquitted.

[547] *Id.*, at 27. "The preparatory acts for the commission of these offenses – in particular the use of digital means to announce, attract the adhesion and active participation of other Internet users to these attacks, anonymise the participants, and claim the success of such attacks – are constitutive of the material element of the offense of a participation in a group formed or an agreement established with a view to the preparation of the offenses referred to above and do not characterize the aggravating circumstance of a '*bande organisée*"'.

In 2011, the Spanish police announced the arrest of the "dome" of the Spanish cell of Anonymous.[548] The statement released to the press suggested the existence of a stable hierarchy in the network, or at least in the Spanish channels of the collective. In fact, aside from a *"delito continuado de daños"*, the defendants were charged with participating in a *"grupo criminal"*, i.e. the broader joint crime offence at the disposal of the Spanish prosecutors. However, in 2016 the *Juzgado de lo Penal of Gijón* acquitted the defendants, as findings did not prove their participation in the activities of Anonymous.[549] This judgment does not provide any analysis of the structural or organisational characteristics of Anonymous, nor any evidence that the group's activities would be covered by any of the various joint crime offences foreseen in the Spanish penal code.

Lastly, two verdicts of the Italian Supreme Court deserve particular attention as they include an interesting analysis of the Anonymous network. At the same time, they exemplify the problems related to the application of criminal association offences on hacker groups. The *Corte suprema di cassazione*, adjudicating two motions challenging pre-trial detention, considered the application of the concept of "*associazione per delinquere"* to the hacktivist collective.[550] In both cases, the Italian Supreme Court upheld the legal basis of the pre-trial detention orders, recognising the existence, within Anonymous, of the organisational and structural features required by the Italian joint crime offence.

The offence of "*associazione per delinquere",* envisaged in Art. 416 of the Italian Penal Code, is a "general" joint crime offence. As defined by the judiciary, it requires a structural organisation, albeit rudimentary, that is functionally key to the commission of an indeterminate series of crimes.[551]

Interestingly, the first approach of the Italian Supreme Court to hacktivism took the form of two parallelisms, evoking previous case law and applying it to other, relatively new, collective criminal phenomena. The first parallelism related to cyber communities attempting to share child pornography online, for which, in 2004, the Italian Supreme Court supported the application of its criminal organisation offence.[552] In this case, the Court highlighted that the community was: *"stabile e organizzata, regolata dalle disposizioni dettate dal promotore e gestore, volta allo scambio ed alla divulgazione, tra gli attuali membri e i futuri aderenti, di foto pedopornografiche"*, and that *"tutti gli aderenti al consortium sceleris siano*

---

[548] Spain, Cuerpo Nacional de Policia, Nota de Prensa, 'La Policía Nacional desarticula la cúpula de la organización "hacktivista" Anonymous en España' (10 June 2011) <http://www.policia.es/prensa/20110610_2.html>.

[549] Spain, Juzgado de lo Penal, Gijón, *Procedimiento Abreviado No 385/15* (6 July 2016).

[550] ITA, Cassazione Penale, *Jugments n. 46156/13 and n. 50620/13.*

[551] Furthermore, the members should be conscious to be part of a stable association and be willing to operate for the fulfillment of the criminal plan. See, *ex plurimis*, ITA, Cassazione Penale, *Judgements n. 20451/13, n. 3886/12; n. 43656/10, n. 21606/09.* See also, e.g., M. Pellissero, *Reati contro la personalità dello stato e contro l'ordine pubblico* (Giappichelli 2010), 249ff.

[552] See ITA, Cassazione Penale, *Judgement n. 50620/13*.

stati edotti dello scopo e delle finalità del gruppo, consistenti nello scambio virtuale di immagini pedopornografiche, condizione per l'ammissione alla comunità virtuale, unitamente all'impegno di inviare periodicamente altre foto."[553]

The second parallelism drew comparison with international terrorism. In Judgment n. 50620/13, on Anonymous, the Supreme Court specified that the minimum level of organisation required by Art. 416 of the Italian Criminal Code is satisfied also in the case of "non-static" organisations: groups operating through relatively autonomous cells linking the various members, associated by a common criminal aim, and operating in non-identifiable locations on the territory. The judgment recalled case-law on international terrorism, where it stated that the requirements of the organised crime offence are satisfied with regard to the: *"strutture cellulari (…) caratterizzate da estrema flessibilità interna, in grado di rimodularsi secondo le pratiche esigenze che, di volta in volta, si presentano, in condizioni di operare anche contemporaneamente in più Stati, ovvero anche in tempi diversi e con contatti fisici, telefonici o comunque a distanza tra gli adepti anche connotati da marcata sporadicità, considerato che i soggetti possono essere arruolati anche di volta in volta, con una sorta di adesione progressiva ed entrano, comunque, a far parte di una struttura associativa saldamente costituita."*[554]

However, it should be pointed out that, in the case of cyber communities that share child pornography, the findings of the Court were related to the stability of the organisation, its structure, the existence of a stable normative set of rules originating from the higher ranks of the group, and the necessity that new members accept the criminal plan of the organisation to be admitted to the community. Such features, conversely, are completely lacking in the case of Anonymous.

On the other hand, international terrorism presents hybrid forms of hierarchy which are substantially different from those of Anonymous. Although flexible, permeable, and decentralised – hierarchies expressed by terrorist groups usually encompass some vertical features, connection between the nodes and, as remarked by the Italian Supreme Court, a *"struttura associativa saldamente costituita"*[555].

---

[553] ITA, Cassazione Penale, *Judgement n. 8296/04.* "Stable and organised, governed by the provisions dictated by the promoter and manager, aimed at the exchange and dissemination, among the current and future members, of child pornography", and that "all members of the *consortium sceleris* have been aware of the purpose and objectives of the group, consisting in the virtual exchange of images related to child abuse: a condition for admission to the virtual community, together with the commitment to regularly send more photos".

[554] ITA, Cassazione Penale, *Judgement n. 31389/08.* "Cells (...) characterised by an extreme internal flexibility, capable of being reshaped according to the practical needs that, from time to time, occur, and to operate simultaneously in multiple states, or also at different times and through physical relations between the members, or by phone or other remote means, even characterised by marked infrequency, considered that the members can also be enrolled from time to time, with a sort of a progressive adhesion to the group, and enter, in any cases, to be part of a firmly established associational structure."

[555] "Firmly established associational structure".

Importantly, the Court suggested that the defendants were operating in particular sections of the network that had a certain degree of cohesion and organisation. Specifically, the Court remarked that: *"non è in discussione la liceità del gruppo Anonymous inteso nella sua dimensione complessiva su scala mondiale, ovvero delle finalità di carattere generale che il gruppo medesimo persegue, ma si discute appunto di cellule che possono avere pianificato iniziative illecite"*.[556] This is of pivotal importance since, in reference to *Anonymous*, certain structural and organisational requirements may only be found in specific areas, and not throughout the whole structure of the network.[557]

However, similarly to other judgments previously examined, the court neither specified the scope of its structural analysis, nor engaged in any considerations on the link between the particular areas of the network covered and its core general structure. Nonetheless, the court advanced some potentially misleading observations about the collective as a whole.

The lens of the Italian Supreme Court rapidly switched from the particular to the general, when it seemed to identify an ideological substratum and an indefinite criminal plan. It failed to note the important differences between these two areas, or the ethereal nature of the link existing between them. Specifically, it was observed that the collective is articulated: *"attraverso la predisposizione del blog ufficiale dell'organizzazione e del video di propaganda, da diffondere sul blog ufficiale; la predisposizione e gestione dei canali di comunicazione IRC privati, che consentono sia la comunicazione diretta fra due soggetti che il dialogo contemporaneo di interi gruppi di persone, in ambito internazionale o nazionale; l'organizzazione, in tali canali, delle linee strategiche; la discussione sulla vulnerabilità dei siti da attaccare; la definizione dei testi di rivendicazione poi diffusi mediante siti web e sulle pagine ufficiali di (omissis); il mantenimento dei contatti con i media e con l'organizzazione (omissis) di livello internazionale; l'effettuazione delle attività di scanning, per verificare la vulnerabilità di possibili siti target, e di exploiting, per accedere abusivamente all'interno dei server che li ospitano; la*

---

[556] ITA, Cassazione Penale, *Judgement n. 50620/13*: "It is not the lawfulness of Anonymous considered in its overall worldwide dimension, or in its general purposes, to be questioned, conversely we are indeed focusing on the cells that may have planned illicit actions."

[557] This is the case, for instance, of a stable associative bond between the members, which can only be found in specific operational areas within the collective. This element is specifically required by the Italian offence, and serves as the distinction element between the crime of criminal association and occasional co-perpetration of crime envisaged by Article 110 of the Italian criminal code. See ITA, Cassazione Penale, *Judgements n. 42635/04 and n. 3340/99*.

progettazione, messa a disposizione e condivisione dei c.d. tools di attacco (programmi deputati ad un determinato compito), che venivano messi a disposizione dell'organizzazione"[558].

Furthermore, the Court stated that: "*un gruppo delimitato di soggetti, per quanto operante in un ambito più vasto nel quale assume di riconoscersi, ben può assurgere ad elemento strutturale di un'associazione rilevante ex art. 416 cod. pen., indipendentemente dall'esistenza di una gerarchia che porti a individuare con certezza chi sia il "capo" del gruppo in questione o se addirittura un vertice esista tout court"*[559].

This analysis seems to draw the requirements of the offence from both the particular and general level of the collective. Such an operation is to be avoided, in the absence of an exhaustive analysis of the peculiar relationship between the operational areas of Anonymous and its general structure. Clearly, this relationship is far from being implicit. The operational levels of the network are not necessarily dependent (from a logical or structural point of view) on the collective general level. Again, the risk arising from such case law is that of creating a dangerous level of criminological confusion.

If it is possible to find, within the overall structure of Anonymous, certain interactions that are provided with the necessary requirements envisaged for a joint crime offence, these areas should be precisely identified. Overextension of the offence to the whole social structure is to be avoided.

---

[558] ITA, Cassazione Penale, *Judgement n. 50620/13*: "Throughout the preparation of the organisation's official blog and the propaganda videos, to be diffused on the official blog; the establishment and management of private IRC communication channels that allow direct communication between two subjects and the contemporary dialogue of entire groups of individuals at the international or national level; the organisation, in these channels, of the strategic guidelines; the discussion on the vulnerabilities of the websites to be attacked; the definition of the claim texts subsequently disseminated on websites and on the official pages of (omitted); maintaining contacts with the media and with the organisation (omitted) at the international level; the scanning operations, in order to check the vulnerabilities of possible target websites, and the exploiting operations, in order to illegally access the servers that host them; the design, provision and sharing of the attack tools (programs aimed to a certain task), which were made available to the organisation."

[559] *Ibid.:* "A limited group of individuals, even if operating in a wider context in which it recognises itself, may satisfy the structural element of the association provided for by Art. 416 Criminal Code, regardless of the existence of a hierarchy that leads to identify the "leader" of such group, or even simply indicating the existence of a leadership."

III PROCEDURAL LAW

"To check who Siri thinks you are, you can ask 'Who am I'?"[560]

[560] J. Centers, *iOS 9: A Take Control Crash Course* (Take Control Books, 2015).

III.I. INTRODUCTION.

A criminal investigation collects information related to a crime to reconstruct its factual history. Traditionally, such information consists of objects or conversations, which need to be retrieved, collected and preserved for their use as evidence. In accordance with the procedural rule of law principle, specific procedural tools are used to protect the rights of the person involved from abuses, and to prevent inaccuracies that will contaminate the validity of the adjudication process.

Today, the investigative landscape is radically changing. Information is increasingly "nonphysical". As of 2018, half of the world population is online.[561] Three billion people use a smartphone.[562] Most traces of their past and present actions, and their communications can be retrieved from their electronic devices or from a server of an ITC.

Information stored in devices, or flowing through the communication process between two machines, are now essential for criminal investigations. In the case of cybercrimes, evidence is mainly in electronic form. Electronic evidence is also increasingly fundamental in relation to ordinary crimes, due to the growing diffusion of digital technology. A suspect or a victim's smartphone may contain important information on their contacts, on their recent communications, on their social connections, on their physical movements, or on their health or financial situation.[563] Essential information can also be extracted, for instance, from their laptop, from their social networks account, from their smart home appliances, or from their car (if equipped with infotainment or event data recorders).

The growing involvement of electronic evidence in all types of crime is likely to revolutionise techniques of investigation, both from a procedural and a forensics point of view.[564]

Specific technical knowledge is necessary to correctly search, intercept, collect, and maintain unaltered digital information. Such information has to be then be analysed and, eventually, this

---

561 See, e.g., 'ITU releases 2018 global and regional ICT estimates: For the first time, more than half of the world's population is using the Internet (ITU, 7 December 2018) <https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx>.

562 See, e.g., 'Number of smartphone users worldwide from 2016 to 2021 (in billions)' (Statista, 26 June 2019) <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.

563 See, e.g., A. Brown, 'This is how much your smartphone knows about you right now' (Express, 7 May 2016).

564 See UNODC, *Comprehensive Study on Cybercrime* (n 66), 118.

analysis should be presented in court. Dedicated training for conventional police forces, or the creation of specific cyber divisions within law enforcement agencies, may be needed to provide them with the necessary technical abilities to deal with electronic evidence.[565]

Furthermore, specific legal provisions may be required to guarantee the accuracy and efficacy of electronic evidence collection, provide binding requirements for the admissibility of evidence on trial, and avoid issues related to possible technical errors, malfunction, or fabrication.[566] Such provisions need to address the specific technical features of digital technology and, in particular, the volatile nature of data.[567] For instance, measures aimed at expedited preservation of data may be necessary to avoid essential data being moved, modified or erased before collection.[568]

Cyber specific procedural provisions should also invest the authorities with the required powers to obtain data from their owners, or from private parties which may be controlling them (in particular, ITCs). Due to the worldwide territorial scope of cyberspace, investigations often extend beyond the relevant State's territory. The proceeding authority may need the cooperation of other States, or private entities controlling the required information. In some cases, national authorities may try to either cooperate exclusively with the ITC, or avoid cooperation by accessing the data autonomously, thus circumventing international cooperation mechanisms. Extraterritorial investigations and, more generally, the framework governing cyber specific cooperation mechanisms will be analysed in the next chapter.

Moreover, there are important issues concerning the rights of a suspect in a cyber investigation. In accordance with the rule of law and its corollaries, specific safeguards and a sharp scope of application of cyber investigation techniques are essential to avoid erroneous, excessive, or abusive use of new types of technology by law enforcement agencies. Cyber criminal procedure must ensure an adequate balance between the investigative needs and the fundamental rights of the persons involved.

---

565 See F. Calderoni, 'The European legal framework on cybercrime: striving for an effective implementation', (2010) 54 Crime, Law and Social Change 339, 340; R. G. Smith, P. Grabosky and G. Urbas, *Cyber Criminals on Trial* (CUP 2004), 152.

566 I. Walden, 'Addressing the Data Problem: The Legal Framework Governing Forensics in an Online Environment', in C. Jensen, S. Poslad, T. Dimitrakos (Eds), *Trust Management* (iTrust 2004), 2.

567 See, *inter alia*, UNODC, *Comprehensive Study on Cybercrime* (n 66), 122; See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 31.

568 Nevertheless, in comparison to substantive cybercrime law, its procedural counterpart is somehow neglected. Its evolution did not take the steady path of the criminalisation of the cyber offences. Most of the States did not have, for a long time, a specific procedural framework aimed at regulating cyber investigations and collection of electronic evidence. Notwithstanding the fact that most traditional procedural provisions do not accurately translate into cyberspace: they were mainly created for tangible objects (*res materiales*), or different technologies, such as telephone communications.

Cyber investigations may be particularly intrusive in the human rights of the suspect, in particular, in their privacy rights, which are increasingly at risk in the age of digital technology. Operating on digital technology may involve a higher amount of personal information than searching a house or intercepting a person's letters.[569]

Technological evolution is changing the balance between opposing interests underlying investigative measures.[570] This relationship appears to be corrupted by a delay of the legislator in keeping up with technological advancement. In particular, this "law lag"[571] may affect the possibility for law enforcement agencies to use new investigative tools. Or, on the other hand, it may induce their use in the absence of a precise legal basis. In the latter case, the suspect is deprived of sufficient safeguards to avoid undue interference with his/her fundamental rights.

This chapter analyses how domestic systems are addressing the issues mentioned above. Particular attention will be devoted to the CoE Convention on Cybercrime, which played a pivotal role in stimulating the creation of a cyber criminal procedure within its territorial scope. Furthermore, it addresses the use of new techniques of cyber investigation, which are not considered by any international instrument. States now have extraordinarily powerful investigative tools at their disposal. For instance, most European States are routinely using hacking or facial recognition techniques for investigations.

III.I.I. ELECTRONIC DATA AS EVIDENCE.

Generally speaking, the objects of a cyber investigation are data. Article 1 of the Budapest Convention provides a general definition of "computer data" – built upon the ISO-definition of data[572]. According to this Article, computer data are "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable

---

[569] Indeed, the principle of proportionality – which mandates an appropriate balance between respect for individual rights and investigative powers – and the principle of procedural legality – which requires a legal basis for infringement of qualified rights, such as the right to privacy – often do not constitute a sufficient limit to the State's power. Broad interpretations of the procedural norms, especially in systems not envisaging exclusionary rules for illegally or improperly obtained evidence, are diffused. See e.g. S. C. Thaman (ed), *Exclusionary Rules in Comparative Law* (Springer Science & Business Media 2012).

[570] Also, in terms of defence rights (see M. Simonato, 'Defence rights and the use of information technology in criminal procedure', (2014) 85 Revue Internationale de Droit Pénal 261.

[571] See D. Mercer, "Technology and the law: dealing with the 'law lag'" (TheAustralian, 4 July 2011), available at: http://www.theaustralian.com.au/archive/business/technology-and-the-law-dealing-with-the-law-lag/news-story/b312d05074f757b67cfbe74d9d85615c.

[572] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 5.

to cause a computer system to perform a function". This definition is applicable both at the procedural level (e.g. in a search and seizure of stored computer data) and the substantive level of the Convention (i.e. as a material element of the offences listed therein).[573]

Once admitted at trial, data becomes "electronic evidence". According to one of the most diffused doctrinal definitions,[574] electronic evidence can be described as "data (comprising the output of analogue devices or data in digital format)[575] that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication."[576] Electronic evidence is thus data which, provided their probative value and their admissibility to the trial, can be used as part of the process of adjudication.[577]

Different types of data can be relevant in a trial. A primary classification, which has already been considered in the previous chapter[578], distinguishes between "static data" – which are data stored in hardware (e.g. a computer, a smartphone, or a server), possessed by the data owner or controlled by a third party – and "fluid", or "transient data", which are data in the process of being transmitted between two hardware devices.[579]

Data can also be categorised according to their nature. "Content data" relate to the actual substance of communication or data processed, stored, or transmitted. Conversely, "metadata" provide information about a communication (traffic data), the location of a device (location data), or a user's basic registration information (subscriber data).[580]

In the Budapest Convention, traffic data are defined by Article 1 (d) as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

---

573 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §25.

574 See S. Mason (ed), *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths 2007).

575 Mason distinguishes between "electronic" and "digital" evidence: the former comprising the latter. The term "electronic evidence" is meant to be broader than mere electronic evidence, also comprising data coming from analogous devices, such as audiotapes or photographic films, which - not originally in digital format - can be digitalised.

576 See S. Mason (ed), *Electronic Evidence: Disclosure, Discovery & Admissibility* (n 574), 9.

577 See, on the definition of digital or electronic evidence, M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci and Fabrizio Turc, *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018), 173ff.

578 See *supra* § II.IV.I.

579 I. Walden, 'Addressing the Data Problem: The Legal Framework Governing Forensics in an Online Environment' (n 566).

580 See, *inter alia*, A. Acquisti, S. di Vimercati and S. Grtizaliset (Eds), *Digital privacy: theory, technologies, and practices* (CRC Press 2007), 423; I. Walden, 'Addressing the Data Problem: The Legal Framework Governing Forensics in an Online Environment' (n 566), 11ff.

Subscriber data is defined by Article 18.3 as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a) the type of communication service used, the technical provisions taken thereto and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement." This type of data may be instrumental to the identification of a subscriber's identity and the services or technical measures used by him/her.[581] Interestingly, the Explanatory Report attached to the Convention specifies that the measures contained therein do not impose upon ITCs any obligation to ensure the correctness of data stored, nor to resist the use of pseudonyms.[582]

The Convention does not define location data. This lack is likely due to the limited diffusion of mobile devices at the time of its adoption. At least partially, subscriber data may cover information on the location of the device.[583]

These various types of data may be subject to different legal regimes. While static data can be searched and seized, transient data should be intercepted. Metadata (more than content data) are usually in possession of an ITC. The collection of data may thus require the cooperation of these private entities.

Furthermore, content data has often been regarded as more sensitive than metadata, since the latter does not disclose the substance of a communication.[584] This distinction is contested, and gradually disappearing. Metadata increasingly provide person-specific information: e.g. social network connections, websites visited (therefore hinting at its content), location at a specific moment, or personal information given in the moment of subscribing to a service.

---

[581] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 178.

[582] *Id.,* § 181.

[583] *Id.,* § 180: "Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available based on the service agreement or arrangement."

[584] See, e.g., ECtHR, *PG and JH v. UK* (Application n. 44787/98), 25 September 2001.

Today, collection of particular types of metadata – e.g. location data, which permit precise geolocation[585] of a device – appears to generate serious privacy issues.[586] Furthermore, various types of metadata combined may allow a reasonably accurate depiction of a person's life. In the oft-cited Digital Rights Ireland Case, annulling the 2006 EU Directive on Data Retention, the Court of Justice of the European Union examined the impact of metadata on the right to privacy.[587] It held that such data "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[588]

---

[585] Geolocation is the identification of the geographic location of an Internet-connected device. One of the primary methods of geolocation is through an IP addresses, a set of binary numbers assigned to each device connected to the web, which indicates its identity and location addressing.

[586] See CoE, Venice Commission Opinion, *Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts* (No. 839/2016), § 26.

[587] ECtHR, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Grand Chambre, Joined Cases C293/12 and C594/12), 8 April 2014.

[588] CJEU, *Cases C-293/12 and C-594/12*, 8 April 2014, §27.

III.II. THE INTERNATIONAL FRAMEWORK ON CYBER INVESTIGATIONS.

In the international cybercrime instruments, procedural issues did not receive the same consideration of the substantive regulation of cyber offences. The CoE Report accompanying Recommendation No. R (89) 9, which dedicated significant attention to the definition of cyber offences, merely considered that "in all industrialized countries until now, the legal discussion on computer crime focused on substantive law and neglected procedural law aspects" and that "only a few countries have enacted new legal provisions concerning investigations in computerised environments".[589] It also noticed that computer-generated evidence and the related legal problems "are relevant not only to the prosecution of computer crime but to all kinds of criminal investigations in computerized environments".[590] The CoE Report gave a first overview of three topics, in order to "initiate a more extensive international discussion"[591]: the coercive powers of law enforcement authorities to gather evidence; the specific legal problems of gathering, storing and linking personal data in criminal proceedings; and the admissibility of evidence consisting of computer records in criminal court proceedings. The CoE Report pointed out both the particular needs of cyber investigations and the problems in applying traditional procedural norms to electronic evidence. However, it omitted to provide any precise recommendations on necessary amendments to Member States' procedural laws.

The problems of criminal procedural law related to information technology were the object of a subsequent CoE Recommendation (No. R [95] 13), which urged "the governments of member states: when reviewing their internal legislation and practice, to be guided by the principles appended to this recommendation"[592]. This Recommendation set forth a series of general principles regarding the search and seizure of data, technical surveillance, the obligation of persons to cooperate with investigating authorities, preservation of electronic evidence, and use

---

589 CoE, *Recommendation No. R (89) 9 on Computer-related crime* (n 60), 69.

590 *Id.,* 69.

591 *Id.,* 70.

592 CoE, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law* (n 63), 2.

of encryption.[593] However, at the domestic level, the 1995 CoE Recommendation's general guidelines did not receive positive implementation.

The CoE Budapest Convention was the first instrument envisaging direct obligations to improve ICT related investigations through cyber-specific powers and measures tailored to the peculiarities of electronic evidence.[594] The provisions contained in the Convention represent a minimum level of harmonisation, as the Convention does not prevent States from enacting cyber-specific investigative tools other than those envisaged therein. The Convention also remains the only European cyber specific criminal instrument envisaging a comprehensive procedural framework. Both the EU instruments on cyberattacks, in fact, do not address procedural law.

III.II.II. THE COE CONVENTION ON CYBERCRIME AND ITS PROCEDURAL PROVISIONS.

The Cybercrime Convention envisages a series of procedural measures aimed at addressing the challenges faced by the investigative authorities concerning electronic evidence. These procedural measures are: expedited preservation of stored computer data (Article 16); expedited preservation and partial disclosure of traffic data (Article 17); production order to a person or a service provider (Article 18); search and seizure of stored computer data (Article 19); real-time collection of traffic data (Article 20); and interception of content data (Article 21). Importantly, these powers and procedures extend beyond the mere substantive scope delineated by the Convention. Article 14 states that each Party shall apply these powers and procedures to the criminal offences established under the Convention and, more in general, to all criminal offences committed by means of a computer system and to the collection of evidence in electronic form of traditional criminal offences. Exceptions *rationae materiae* are provided in relation to Article 20 and 21 (real-time collection of traffic data, and interception of content data), and will be analysed further, in the sections about those provisions.

---

593 Two further points address research, statistic and training, and international cooperation.

594 See D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (2004) 18 International Review of Law, Computers & Technology 165, 166.

Preservation order.

Electronic evidence consistently differs from traditional evidence. Having a tangible form, physical evidence is, in most cases, difficult to alter without leaving traces. Conversely, data are extremely volatile and can be manipulated within seconds. A series of specific procedural measures are thus necessary to prevent alteration or erasure of data.

A preservation measure naturally targets data holders, such as ITCs. Data holders store data for a limited amount of time, since storage requires economic and technical resources. Furthermore, specific storage time-limits can be mandated by data retention and protection norms.[595] Investigative authorities therefore have a particular need to preserve and protect the integrity of data before their seizure, to ensure that their evidentiary integrity is maintained for potential use in trial, and to avoid untimely erasure.[596] A provisional order requires the holder to provisionally "freeze" data to avoid their erasure. It temporarily allows the authorities to prepare and obtain the subsequent seizure or production, while at the same time safeguarding the integrity of the data sought.[597]

It is essential to distinguish between the preservation and the retention of data. Data retention provisions are administrative, general obligations, requiring communication providers to retain specific data for a certain amount of time.[598] Such provisions may mandate the keeping of data already generated in the holder's possession, temporally limit it, or prohibit the retention of particular types of data. Retention regulations may work as a substitute for preservation, as they dictate that the holder of data must keep data for a certain amount of time.[599] Furthermore, the two measures may work in parallel or combination. A data retention obligation can extend the amount of time for which data is available and, when combined with prevention order, may augment this period.[600]

---

595 UNODC, *Comprehensive Study on Cybercrime* (n 66), 127; see also supra, at xxx.

596 See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 46. See also D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 168.

597 CoE, Cybercrime Convention Committee, *Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, T-CY (2012)10, (2012), 6.

598 See A. Vedaschi and V. Lubello, 'Data retention and its implications for the fundamental right to privacy: A European perspective' (2015) 20 Tilburg Law Review 14; D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 168; CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 151.

599 See CoE, Cybercrime Convention Committee, *Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (n 597), 8, 9.

600 *Id.,* 75.

Data preservation orders are investigative tools specifically constructed to deal with the particularities of electronic data. They are entirely cyber specific and have no analogous counterpart amongst the traditional investigative powers. Several multilateral cybercrime instruments envisage preservation measures.[601] Among them, the CoE Convention regulates expedited preservation of data in Articles 16 and 17.[602]

The need to preserve data can be satisfied through a direct seizure of data upon the search of the holder premises, or a production order (examined *infra*).[603] Article 16 of the CoE Convention uses the syntagma to "order or similarly obtain" data, which is intended to contemplate different means of obtaining preservation apart from a preservation order.[604]

However, the specificity of the preservation orders may afford preferable applicative conditions. In comparison with the alternative investigative tools, a preservation order is more expeditious and less onerous. In particular, it avoids the disruption of activities and reputation of the private party holding data.[605] Moreover, the alternative measures may have higher requirements in terms of justification and judicial authorisation and may involve the disclosure of the measure to the suspect.

However, the CoE Assessment Report on the implementation of the preservation provisions of the Budapest Convention noted that several States Parties did not enact specific frameworks envisaging preservation orders. Conversely, many States relied on traditional powers and measures to preserve electronic evidence.[606] In the German system, for instance, according to Sections 94 and 98 of the Code of Criminal Procedure, preservation can be obtained by seizing the storage media.

In some cases, preservation is obtained through arrangements, or administrative measures, which regulate cooperation between ITCs and investigative authorities.[607] This method appears in line with the obligation stemming from the CoE Convention, which requires the Parties to "adopt such legislative *and other measures*"[608] to obtain preservation. It could be contested,

---

601 See, e.g. LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Art. 23.

602 The Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law (*supra* n 63) did not envisage such a measure.

603 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 155.

604 *Id.*, § 165

605 …of particular importance when the holder is a trustworthy, legitimate business. See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 155.

606 See CoE, Cybercrime Convention Committee, *Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (n 597), 7.

607 *Id.,* 8.

608 Italics added.

however, that the use of non-legislative measures should, in any case, be complementary or subordinated to a legal process, in order to permit an assessment of the proportionality between the measure and the rights of the individuals involved. [609]

As pointed out in the Assessment Report, inconsistencies emerged during the Cybercrime Convention Committee Plenary about the content of Article 16 of the Budapest Convention. In particular, the Parties to the Convention had different views on whether the use of powers such as search, seizure, or production orders, was in line with this provision. The report highlights the importance of the temporal element in avoiding the alteration of data. Consequently, it points out that, to meet the requirements of the provision, the use of alternative measures must in any case allow for the securing of all types of data in an expedited manner.[610]

Additionally, most Parties to the CoE Convention reported that – notwithstanding the existence of domestic preservation measures – search and seizure provisions or production orders are often preferred. An exception exists in cases of international assistance requests, where domestic judicial orders for search, seizure, or production of data are more difficult to obtain. [611]

The material scope of application of Article 16 and 17 of the CoE Convention is "computer data, including traffic data, that has been stored by means of a computer system", in particular "where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." The object of the preservation order is, therefore, any type of stored data.

The order to preserve is directed to the natural or legal person that is in possession of or control over the relevant data. Confidentiality of the data holder may be necessary in order to avoid contamination or destruction of further evidence by the suspect. Therefore, according to the CoE Convention's provisions, the domestic measure shall "oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law".[612]

---

609 Cfr inter alia ECtHR, Leander v Sweden, Application n. 9248/81, 26 March 1987, recognizing that mere storage of information about an individual may amount to an interference with their private life.

610 See CoE, Cybercrime Convention Committee, *Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (n 597), note 7.

611 *Id.,* 10ff. At least, outside the European common area of freedom, security and justice, where international assistance is requested and executed through the European Investigation Order, and thus informed by the principle of expeditious and extended mutual recognition (see EU, *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*, OJ L 130, 1.5.2014).

612 CoE, *Convention on Cybercrime* (n 81), Article 16 § 3.

Neither of the Articles contains a definition of "preservation" which specifies how the data should be preserved. The actual means of preservation are thus left to the State to determine.[613] Therefore, States can decide to envisage the complete freezing of data, which render them inaccessible to the owner. However, this procedure may be an indicator of ongoing investigations, and are therefore likely to alert the suspect.

The articles specify time limits for preservation: data should be preserved as long as necessary, up to a maximum of 90 days. The order may be renewable in order to allow subsequent production orders or seizures by the competent authorities.

The domestic provisions introduced on the basis of Article 16 and 17 may be activated through a mutual assistance request coming from another Party, as provided for by Article 29 and 30 of the Convention, which regulate the expedited preservation of data following a mutual assistance request. However, in such a case, the preservation shall be for not less than 60 days. The existence of a legal power to order preservation is thus essential both for domestic investigations and for third countries seeking international cooperation, the investigation of which could be frustrated if the requested State is unable to preserve data expeditiously.[614]

Article 17 concerns preservation and partial disclosure of traffic data. Such a type of data may be critical for determining the source or destination of a communication.[615] Traffic data presents two main problematic traits. Firstly, according to data retention laws, traffic data is usually stored for a short period. Secondly, and most importantly, more than one ITC may be involved in each communication.[616] Hence, a single ITC may possess only "one piece of the puzzle", and not hold enough data to determine the origin or destination of the entire communication. Article 17 is therefore aimed at affecting all entities that take part in the chain of communication. However, the Article requires States to "ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication", without specifying the procedural means to achieve it. For instance, the State may either serve separate orders on each provider, or serve

---

[613] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 46.

[614] UNODC, *Comprehensive Study on Cybercrime* (n 66), 128.

[615] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), 165.

[616] D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 168; L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 47.

a single order the scope of which covers all providers involved, i.e. that took part (or is eventually identified as having taken part) in the communication.[617]

Furthermore, Article 17 requires the expeditious disclosure to the competent authority "of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted". Traffic data is not disclosed to the competent authorities until a production order is served, or other measures aimed to obtain data are taken. Partial disclosure may therefore allow knowledge of whether the service provider possesses all of the relevant traffic data, or conversely other providers were involved in the communication. This allows immediate reconstruction of the chain of communication and its full traceability. If the communication involves a foreign provider, investigative authorities shall request assistance according to the rules of international cooperation.[618]

Preservation is a provisional measure aimed at ensuring evidence integrity. Therefore, it is meant to be complemented by subsequent measures aimed at obtaining data preserved, such as a production order.[619]

Production order.

Once stored data are identified, and possibly preserved as a result of a preservation measure, they have to be acquired by the investigation authorities. Provisions regulating orders for production of data grant the legal power to request and obtain existing stored data from the person possessing or controlling it.

Several international instruments on cybercrime contain provisions regulating production orders.[620] The CoE Convention addresses such measure at Article 18.[621]

The obligation stemming from Article 18 of the CoE Convention can be fulfilled by amending "traditional" production orders to include the production of data. Indeed, this is the solution adopted by most European States. For instance, Article 60-1 of the French Criminal Procedure Code enables the "*procureur de la République*" or "*l'officier de police judiciaire*" to request production of

---

[617] The Explanatory Report to the Convention suggests a third option, consisting of a series of subsequent notifications from the previous to the next service provider of the chain. However, such an option may be weaker, as the direct power of the State, which is the basis of the order to cooperate, may be diluted in a private-to-private relation.

[618] D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 168.

[619] *Ibid.*

[620] See, for instance, LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 25.1.

[621] The Article follows the construction of Article III of the 1995 Recommendation (CoE, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law* (n 63)).

"*informations intéressant l'enquête, y compris celles issues d 'un système informatique ou d'un traitement de données nominatives*".[622]

In other cases, traditional production or document disclosure provisions have a general scope of application that covers data requests.[623] For example, Section 95 of the German Procedural Code, regulating production orders, covers "objects which may be of importance as evidence for the investigation",[624] and can be used to obtain electronic data.

Other investigative measures can produce the same result as production orders. Primarily, competent authorities may rely on the search and seizure of data. However, as already mentioned, such investigative tools can be more onerous (in terms of time and authorisation), and possibly more intrusive in the legitimate activity of the persons involved.[625]

The CoE Convention distinguishes between two types of production orders: first, request aimed at all types of data "stored in a computer system or a computer-data storage medium", and possessed or controlled by a person in the relevant State's territory; second, requests for subscriber information possessed or controlled by a service provider offering its services in the territory of the Party (only data relating to such services). The importance of this material distinction is in its territorial scope. The Explanatory Report to the CoE Convention specifies that "possession or control" indicates both physical possession of data, and situations in which data – although not in their physical possession – are under the legitimate control of the person and can be legally retrieved and produced. This is the case, for instance, when data are stored in remote online storage services. Conversely, mere technical ability to access remotely stored data that is not under legitimate control is to be excluded.[626]

The current diffusion of cloud computing has brought a series of jurisdictional issues related to the enforceability of domestic production orders on service providers located outside the relevant State's territory. In particular, problems may arise for investigative authorities seeking access to: data concerning services offered in the territory, if the service provider is not established therein; and data stored in foreign jurisdictions, or unknown or multiple locations (in

---

[622] FR, *Code de Procédure Pénale*, Article 60-1 (Information on the investigation, included those coming from a computer system or from personal data processing). ITA, *Codice di Procedura Penale*, Article 256, on production orders targeting specific persons (it contains a similar formulation, since its material scope covers "acts and document (…), and data, information" and, quite interestingly "software").

[623] UNODC, *Comprehensive Study on Cybercrime* (n 66), 129.

[624] GER, *Strafprozessordnung*, Article 95.

[625] UNODC, *Comprehensive Study on Cybercrime* (n 66), 128.

[626] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 173

the "cloud"). These issues, which are central to the investigative challenges related to electronic evidence, will be considered in the chapter on international cooperation.

In accordance with the safeguards related to the right to privacy, each Party may prescribe differentiations (e.g. terms of production, authorities issuing the order, or the application to particular types of crimes) concerning different types of data.[627] In Germany, for instance, orders for production of traffic data – regulated by Section 100g *Strafprozeßordnung* – are limited to particularly serious criminal offences and require a court order (although in cases of urgency the order can be issued by a public prosecutor).

Confidentiality may be necessary for the success of the investigation.[628] However, the CoE Convention's provision on production orders does not contain specific references to it. The modalities of production – such as the period for disclosure, or its form – are also left to the discretion of each Party.[629]

A final consideration relates to the specificity of the order. The Explanatory Report to the Convention considers that "as the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings […], production orders are to be used in individual cases concerning, usually, particular subscribers"[630]. The Report thus specifies that Article 18 does not authorise State Parties to issue legal orders to disclose indiscriminate amounts of data about groups of persons, in particular for the purpose of data mining.[631]

Data mining is currently employed as a way to "predict" crime.[632] Crime analysis and prediction software are increasingly used by law enforcement agencies to predict spatial and temporal information relating to possible future crimes. These predictions may even cover the identity of the potential perpetrators. Predictive algorithms can work on numerous types of data, such as crime reports, browser searches, or social media profiles.[633] They enable preventive

---

627 *Id.,* § 174.

628 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 175.

629 *Id.,* § 176.

630 *Id.,* § 182.

631 Data mining is the process of discovering patterns in large data sets. M. Kantardzic, *Data Mining: Concepts, Models, Methods, and Algorithms* (John Wiley & Sons 2019). See also CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 182.

632 See, e.g., C. McCue, *Data mining and predictive analysis: Intelligence gathering and crime analysis* (Butterworth-Heinemann 2014); D. Quick K. R. Choo, 'Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive' (2014) 480 Trends & Issues in Crime and Criminal Justice 1.

633 See M. Hvistendahl, "Can 'predictive policing' prevent crime before it happens?" (28 September 2016, Science) <http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens>.

action in order to stop the crime from being committed or continued.[634] This activity – which brings to mind Philip K. Dick's famous novel "Minority Report" – has encountered numerous ethical and privacy critiques.[635]

The limits to gathering and using large amounts of data to predict crimes do not directly stem from cybercrime conventions. Principally, they are to be found in privacy and data protection regulations. In the EU, Directive 680/2016[636] on the processing of personal data for the purposes of crime prevention, investigation, detection or prosecution, explicitly recognises the need for "competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected". A series of principles and limits to such processing are set in its Article 4. However, these principles and limits are overtly vague. Among them, the pivotal limit to data mining in law enforcement is that gathering of data should be "adequate, relevant and not excessive in relation to the purposes for which they are processed"[637].

Search and seizure.

The search and seizure of data is the most common investigative measure for finding and collecting objects of evidentiary value. Electronic data – being *res immateriales* – are often left uncovered by traditional search and seizure provisions. Hence, digital search and seizure provisions aim to establish an equivalent power with regard to computer systems or storage mediums, and data stored therein. Moreover, they are designed to accommodate the

---

634 See, e.g., J. Jouvenal, 'Is crime prediction software the way forward for modern policing? Or biased against minorities?' (The Independent, 22 November 2016) <http://www.independent.co.uk/news/world/americas/crime-prediction-software-modern-policing-or-biased-against-minorities-us-police-law-a7429676.html>; Predpol official website <www.predpol.com>.

635 See K. Miller, 'Total surveillance, big data, and predictive crime technology:
privacy's perfect storm', (2014) 19 Journal technology of law and policy 105, at 105.
See also Dave Gershgorn, 'Software Used to Predict Crime Can Now Be Scoured for Bias' (Defence One, 23 March 2017) <http://www.defenseone.com/technology/2017/03/software-used-predict-crime-can-now-be-scoured-bias/136426/>.

636 See V. Mitsilegas, *Justice and Trust in the European Legal Order* (Jovene 2016), 172.

637 EU, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, Article 4.

particularities of data. Specifically, they indicate the necessary modalities of copying data and maintaining data integrity.

Several multilateral instruments on cybercrime envisage search and seizure powers.[638] In the CoE Convention, access and search of computer systems and independent data storage media are regulated by Article 19.[639]

The primary scope of digital search and seizure provisions is to extend searching and seizing powers on new technology. This purpose can be obtained by introducing new legal tools exclusively tailored on digital technology. Furthermore, it can be reached by extending the scope of the traditional search and seizure provisions to cover hardware and data. Although the former solution may permit a more precise accommodation of the characteristics of data, States tend to prefer the latter solution. For instance, the French system allows searches on "*papiers, documents, données informatiques ou autres objets*"[640], and documental seizures on "*documents ou des données informatiques*"[641]. The Romanian system envisages that "the provisions of the Criminal Procedure Code regarding searches at home are applied accordingly" on computer systems and data (notwithstanding the existence of specific legislation on cybercrime).[642]

The use of traditional search and seizure models leads to maintaining most of the requirements of the traditional search and seizure, such as the preconditions for obtaining legal authority to undertake a search or a seizure, or the evidentiary grounds required for legal authorization.[643] Important among these requirements are those relating to the target of the measure, which must be sufficiently precise. A search and seizure cannot be a "fishing expedition" on hardware or files beyond those described in the warrant.[644]

If data is not stored in the system, and is only accessible from the searched device (e.g. through the web, or through a link to a storage device), the extension of the search to such areas may be

---

638 See, for instance, LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Articles 26 and 27.

639 Article 19 of the Budapest Convention thus provides for a legal authority comprising both physical and digital searches.

640 FR, *Code de Procédure Pénale,* Article 56 (Documents, electronic data or other objects).

641 *Id.,* Article 97.

642 Romania, *Law n. 161/2003*, Article 56.

643 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 186. See also CoE, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law* (n 63), 2.

644 In the US, such extension may lead to a suppression of all evidence obtained (due to the flagrant disregard of the warrant, and to the famous "fruit of the poisoned tree" doctrine). See, e.g., US, *United States v. Liu*, 239 F.3d 138 (2d Cir. 2000); US, *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996); US, *United States v. Young*, 877 F.2d 1099, 1105-06 (1st Cir. 1989).

envisaged.[645] Where data sought are stored (or partly stored) in another computer system, and are lawfully accessible from or available to the initial system, Article 19 of the CoE Convention requires Parties to empower their investigative authorities to "expeditiously extend the search or similar accessing to the other system". To give an example, Section 110 (3) of the German Code of Criminal Procedure allows the extension of the search to separate storage media insofar as they are accessible from the storage medium (even through the web), and only in cases where there is reason to believe that the data sought would otherwise be lost. However, both hardware and software must be located in the territory of the State. Article 19 does not authorise extraterritorial searches, which should be regulated according to criminal international law. For instance, the extension of the searches to data stored on cloud services may not be allowed.[646]

The issue of the notification of a search procedure is not regulated by the Convention and is left to be determined by domestic law. On this issue, States usually follow the traditional search and seizure scheme. Search and seizure is generally not intended to be a surreptitious measure. Besides notification, the subject of a physical search is usually made aware of its existence by the very nature of it, which impinge on the physical premises of the person. Conversely, in the online world, digital search and seizure may be less apparent. On the other hand, due to the volatility of data, such a notification is more likely to prejudice the investigation. The Explanatory Report to the Convention suggests that, in the existence of such a risk, postponement of the notification could be considered.

Article 19, paragraph 3 addresses subsequent seizure (or similarly securing) of data accessed under paragraphs 1 and 2. Indeed, data – being intangible – cannot be directly seized. Operations to seize data therefore require either a previous seizure of the physical medium on which data are stored[647], a copy of the data in a tangible form (i.e. on paper), or a copy of the data on a physical storage medium to be seized. In the latter case, copies shall be made under

---

[645] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 187. The options, when drafting digital search and seizure provisions, were to maintain traditional terminology ("search" and "seize"); to use new, technologically oriented terms (such as "access", "secure" or "copy"), or to use mixed terms. The CoE Convention adopted the latter solution ("search or similarly access", "seize or similarly secure"). The use of new or traditional terminology is left to the discretion of the State.

[646] See e.g. N. Schultheis, 'Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry' (2014) 9 Brooklyn Journal of Corporate, Financial & Commercial Law 661; S. J. Kohls, 'Searching the Clouds: Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account' (2012) 4 Case Western Reserve Journal of Law, Technology & the Internet 169.

[647] See, on the problems related to the bifurcation of the digital search and seizure into a physical search to seize computer hardware, and a subsequent digital search to obtain data, O. S. Kerr, 'Search Warrants in an Era of Electronic Evidence', (2005) 75 Mississippi Law Journal 85.

specific procedures aimed at guaranteeing correspondence to the original data, inalterability, and integrity of their probative value.

Often, due to time requirements and the complex nature of the procedure, the preferred action is to take over the hardware and conduct in-depth searches in specific labs. In such a case, the activity of the legal or natural persons possessing or controlling the relevant hardware and data may be strongly impaired. The seized medium would likely contain licit information, perhaps unrelated to the case, of which the person would be deprived until restitution.

The Romanian Law n. 161/2003, regulating *inter alia* digital searches and seizures aligned with Article 19 of the Convention, mandates copying data on a physical storage medium to be seized if seizing the hardware containing original data may severely affect the activities performed by the persons possessing it.

In all cases, specific attention is given to avoid alteration of data, in particular in their chain of custody. A modification can easily take place as a result of inexpert handling by law enforcement agencies, which may lead to an alteration of the probative value of the given data (either in favour or against the suspect/accused). When permitted by domestic law, participation in the operations of forensic experts appointed by the defence may be fundamental to preventing the alteration of data.

Article 19.3 (e) of the CoE Convention recognises the need to "maintain the integrity of the relevant stored computer data", although it frames it as a "power". Due to their pivotal importance, and the strict relevance in relation to the most fundamental principles of procedural law, measures aimed at preserving the integrity of seized data are widely adopted. In the Italian system, the general search and seizure powers cover data and computer systems and require modes of operation ensuring conservation, conformity, and inalterability of the copied data.[648]

Besides their evidentiary aim, digital seizures may serve a further preventive purpose of ending or avoiding the commission of an offence, in particular in the case of malware or scam websites. Once identified, Article 19 paragraph 3 envisages the power to "render inaccessible or remove" the sought data, which can be done by blocking access to data or encrypting it. The provision does not outline any specific procedure for preventive seizure. Therefore, probative and preventive seizures will be differently regulated only if the domestic system provide so.[649]

A preventive seizure is not intended to destroy data, but merely to avoid further harmful consequences or reiteration of the crime. Indeed, data can be returned to the owner or

---

[648] ITA, Codice di Procedura Penale, Articles 247, 254bis and 353.

[649] Typically, preventive measures require a higher standard for application, such as approval by a judge.

controller following the outcome of the trial.[650] The French system, in Article 97 of the Code of Criminal Procedure, allows the destruction of the original data whose use or detention is "*illégal ou dangereux pour la sécurité des personnes ou des biens*"[651] only if a copy of such data has been realised.
Article 19 paragraph 4 envisages a coercive measure to compel "any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein" (i.e. the system administrator) to cooperate with the investigating authorities by providing the necessary information to enable the undertaking of the digital search and seizure. The limits of this measure are restricted to what "is reasonable". The criteria of "reasonableness" is extremely vague. In all likelihood, it comprises disclosing passwords or keys concerning existing security measures to the investigating authorities. Although the Convention does not deal explicitly with this matter, this provision may include the obligation to decrypt encrypted data or to disclose encryption keys. It is unclear whether the system administrator could oppose privacy concerns related to other users or to data not authorised to be searched.[652]
The duty to protect data rests upon the data controller in light of both the contractual norms in force between the data holder and the users, and data regulation provisions. In the EU, Regulation 679/2016 imposes on the data controller a duty to notify any personal data breach to the supervisory authority and envisage its liability for any infringement of the Regulation. It is interesting to see how the application of the Regulation will impacts on enforceable limits to investigations. It is likely that Data Protection Officers ("DPOs") will be inserted into the bilateral relationship between the system administrators and the investigation authority. According to the Regulation, DPOs should be "involved, properly and in a timely manner, in all issues which relate to the protection of personal data".
A system administrator possesses particular knowledge of the searched computer system and the possible security measures presented by the case. His/her participation may facilitate the search and seizure of data, enhancing their efficacy in cost and time. By accelerating the operations, their help may also be beneficial for the persons involved.[653]
The provision on the system administrator's cooperation is scarcely implemented. Article 88 of the Belgian Code of Criminal Procedure envisages such a cooperation order but does not

---

[650] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 189. Cfr D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 169.

[651] "Illegal or dangerous to the safety of people or goods".

[652] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 202.

[653] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 201.

provide for any reasonable refusal condition. Furthermore, it envisages an offence punishing those who refuse to cooperate with or hinder the search. [654]

Interception.

The investigative measures that have been analysed so far target static data and are aimed at preserving, retrieving, or collecting them. Conversely, transient data must be intercepted "in real-time" during the communication process.

Several international cyber-specific instruments envisage provisions on the real-time collection of data.[655] A distinction is usually made between collection of traffic and content data, with different legal prerequisites to authorisation. Such a distinction is mainly related to presumed variation in invasiveness in the private life of the persons involved between these two kinds of data.[656]

In the CoE system, interception of data was firstly addressed by Recommendation No. R (95) 13. The Recommendation advocated a review of the domestic criminal procedures to allow for the interception of telecommunications and the collection of traffic data. Recognising the related privacy concerns, the Recommendation suggested a limitation of its use for serious offences against the confidentiality, integrity, and availability of telecommunication or computer systems.

Due to the diffusion of digital technology, digital evidence became increasingly pivotal in ordinary, non-technological crimes. The CoE Convention on Cybercrime regulates "real-time collection of traffic data" and "real-time interception of content data" – at Articles 20 and 21 respectively – without following the qualitative limitation found in the CoE Recommendation.

Concerning content data, Article 21 limits their collection to "a range of serious offences to be determined by domestic law", following the principle of proportionality. Usually, domestic systems limit the scope of the measure either to a specific list of offences or categories of offences, or to offences punished with a certain amount of detention (similar to the interception of telephone communication).

---

654 Belgium, *Code d'Instruction Criminelle / Wetboek van Strafvordering*, Article 88: "celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement".

655 See, e.g., LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Artt. 28 and 29.

656 See UNODC, *Comprehensive Study on Cybercrime* (n 66), 130; D. Cangemi, 'Procedural law provisions of the Council of Europe Convention on cybercrime' (n 594), 170.

At the time of drafting the Convention, traffic data were considered to have a marginal effect upon privacy interests. According to paragraph 3 of Article 14, a Party may reserve the right to apply Article 20 only to offences or categories of offences specified in the reservation. The Article forbids stricter restriction than "the range of offences to which (the State) applies the measure of interception of content data". Furthermore, it suggests avoiding the use of such a reservation to enable the broadest possible range within which traffic data can be collected. This approach may have been deprived of its rationale. Indeed, today traffic data ("metadata") can provide the investigative authorities with particularly sensitive information about a user.

States usually regulate real-time data collection without specifying the data type. Few systems envisage among their investigative tools a specific provision on real-time collection of traffic data.[657] The German system provides at Section 100g of the Criminal Procedure Code the possibility to collect traffic data "to the extent that this is necessary to establish the facts or determine the accused's whereabouts". The scope of this Section is limited to investigations into serious offences, or cybercrimes. In the latter case, according to the principle of proportionality, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success, and if the acquisition of the data is proportionate to the seriousness of the case.

Commonly, telecommunication interceptions follow the same *rationae materiae* restrictions envisaged in the domestic system for traditional criminal surveillance. In most cases, due to their internal relations with digital evidence, the material scope of these interceptions also extends to cybercrimes.[658]

Both provisions on real-time data collection envisaged by the CoE Convention require data to be associated with "specified communications" transmitted by a computer system. Hence, data targeted must be explicitly indicated in the authorisation to intercept. Indiscriminate surveillance, or "fishing expeditions" to discover crimes, are precluded.[659] However, the limits to the scope of data collection are to be found in privacy legislations.

Articles 20 and 21 address both interceptions by the investigative authorities and autonomous collection by service providers. They require State parties to provide their investigative authorities with the capacity to collect or record data by technical means, and to compel service providers to collect or record data directly, or to cooperate with or assist the authorities in doing

---

[657] See L. Picotti and I. Salvadori, *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices* (n 197), 50.

[658] In the Italian system, for instance, Article 266bis of the Code of Criminal Procedure limits interception of communication to crimes for which traditional interception is allowed, and to cybercrimes.

[659] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 219.

so.[660] No obligation is set out by the Convention regarding the technological means to be employed to this end. Further, the Convention does not oblige service providers to equip themselves with technical capabilities allowing them to collect, record, cooperate, or assist.[661]

The articles also specify the territorial application of the interception measures. They require that communications targeted must be "in the territory of the Party". This clause will likely cover physical infrastructures or devices located on the territory of the State, even if the communication only passes through them.[662] International cooperation mechanisms in force between the parties may provide otherwise, permitting extraterritoriality, as it will be considered *infra.*

Traditionally, interception is a hidden investigative measure. Since knowledge of the measure by the targeted person will frustrate its efficacy, interception does not mandate the notification of persons involved. Additionally, Articles 20 and 21 of the CoE Convention envisage an obligation of secrecy for ITCs involved, which must keep the fact of the execution of these investigative measures, and any information about it, strictly confidential. Such provisions are aimed at keeping interceptions surreptitious and relieving the service provider of any contractual or other types of obligation towards their clients.[663] As correctly noted by the Explanatory Report to the Convention, confidentiality can also be ensured using other legal tools, such as preventing disclosure of information about the interception through the offence of obstruction of justice.[664]

Secrecy is indeed one of the fundamental characteristics of interception. From secrecy follows its particular invasiveness. Its invisibility undermines its accountability. The indiscriminate and abusive use of electronic wiretapping by totalitarian regimes and democratic countries alike – testified by notorious cases such as the warrantless surveillance by the NSA[665] – has generated the fear of constant State surveillance and calls for stringent privacy protections against the investigative activities of the State.[666]

---

[660] For instance, according to FR, *Code des postes et des communications électroniques*, Article D98-7-III, ITCs are required to implement the measures necessary to allow interception.

[661] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 220. The issue of cooperation between States and ITCs, due to its sensibility, will be addressed in Chapter 4 – Jurisdiction and International Cooperation.

[662] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 222.

[663] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 226.

[664] *Ibid.*

[665] See The Guardian, The NSA Files <https://www.theguardian.com/us-news/the-nsa-files>.

[666] See B. Whitfield Diffie and S. Landau, *Privacy on the line: the politics of wiretapping and encryption* (MIT Press 2017), 4.

III.II.I. STATIC OR TRANSIENT DATA? THE SEIZURE OR INTERCEPTION "DILEMMA".

A fundamental aspect of data classification pertains to their "status" at the moment of collection. The type of investigative measures to be applied, and the related legal requisites for application, are strictly related this status. Static data, stored in hardware, can be subject to seizure. Conversely, transient data, in the process of transmission between hardware, can only be collected in "real-time" on the basis of the provisions regulating interception.

The distinction between static and transient data is of utmost importance. From this distinction follows the application of seizure or interception measures, which are differently regulated. Interception usually demands stricter requirements than seizure, due to a higher impact on the privacy rights of the persons involved.

The 1995 CoE Recommendation recognised the relevance of this problem, suggesting that "the legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied". However, the CoE Convention did not address the issue. A certain degree of blurring between the two legal categories still exists.

In the concrete application of the cyber investigatory measures on online communications, issues related to the distinction between static and transient data initially emerged with regard to emails. Today, due to the enormous proliferation of communication applications for mobile devices, the same problems can be transposed to numerous types of digital communications, such as SMS, chats, or voice messages.

Emails are created in the sender's device, then transmitted to the ISP server. They are then sent to the recipient's mailbox server, and finally received by the recipient. The message can thus be acquired at several locations: during input in the sender's keyboard (or through the microphone, if a voice recognition software is used), on his/her device, on the path to the ISP, in the ISP or mailbox's server, on the path to the recipient, and on his/her device.

Based on a linear application of the "static/transient" dichotomy, messages can be "intercepted" during input in the device, during transmission between servers, or between the second server and the recipient. Likewise, they can be "seized" when stored in the origin and destination devices. A significant problem may arise when data is only temporarily stored in the ISP's and mailbox server during transit. This issue remains something of a grey area and may receive different interpretations when considered in different ways.

Communications can be perceived as monistic entities, without taking into consideration the intermediate steps not involving the sender and recipient. The path from the sender to the recipient is merely considered as a flux of information in transit. As data in transit, they can only be subject to interception.

This is the approach used by the Australian Telecommunications Interception Act, for instance. According to the Act, "a communication is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication, and is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication".[667] The Act thus allows interception of communications passing over a telecommunications system even if it is temporarily stored there. A seizure can be only operated when data has completed the passage through the telecommunications system. Interestingly, when data is received by the recipient (thus ending its path), a seizure may be operated both on the recipient's device, or in the ISP's server in case a copy is still there.

This approach generates problems in cases where there are delays in the ISP's servers or if the message does not reach the recipient. The message, although theoretically "in transit", remains static on a server. In such a case, it is unclear if the investigation authorities are to apply seizure or interception measures.

A similar approach to digital messages in transit – subjecting the whole path to the interception discipline – was suggested in the Italian system.[668] However, in 2008, Article 254 of the Italian *Codice di Procedura Penale* – regulating seizure of postal correspondence – was amended in order to allow direct seizure on ISPs' servers of "correspondence sent via digital means". The amendment (adopted in fulfilment of the obligations stemming from the CoE Convention) thus expresses a formal equivalence between digital and physical correspondence. Just as postal correspondence necessarily stops in its path from the sender to the recipient at intermediary mail offices, where it can be seized, digital messages temporarily stored in servers can be subject to seizure. Importantly, the search should be specific in targeting data already stored in the

---

667 See Australia, *1979 Australian Telecommunications Interception Act*, §5F. See also S. Ramage, *Privacy-Law of Civil Liberties* (iUniverse, 2007); Electronic Frontier Australia, "Telecommunications Interception Legislation Amendment Bill 2002" <https://www.efa.org.au/Issues/Privacy/tia_bill2002.html#existing> on the proposed 2002 Telecommunications Interception Legislation Amendment Bill, that would have allowed investigative authorities to seize communications passing over a telecommunications system that are delayed or stored in transit.

668 See R. Orlandi, 'Questioni attuali in tema di processo penale e informatica', (2009) 1 Rivista di Diritto Processuale 129, 135.

server, and not aimed at anticipating the arrival of messages "in route" to the server from a specific sender. In such a case, the seizure masks a substantial interception of data.[669]

Further considerations may even advocate a complete exclusion of the possibility to intercept digital communications.[670] Contrary to the traditional objects of interception, in the moment of their apprehension digital messages are already entirely formed.[671] Being mediated by technology, this type of human-to-human interaction is not exhausted in a simultaneous divulgence and apprehension. Instead, it is necessarily fixed in a medium that travels to the recipient, conveying the sender's message.

The underlying ratio of interception is the ephemerality of a private message. Such ephemerality legitimates the resort to an investigational measure capable of a hidden real-time caption of a message during the process of formation. Conversely, when a message is already crystallised in the probative value, the investigative measure adopted will be seizure, which requires different requisites and the notification of the operation to the persons involved.

The "static/transient" dichotomy seems unable to fully represent digital communications, and satisfyingly guide their investigative collection. Grey areas persist.

In the absence of a fresh approach, such gaps are usually filled via resort to analogy, which is not desirable. Digital technology presents peculiar traits not expressed by its "physical counterparts". Analogy may therefore lead to a limited understanding of matters and unsatisfactory solutions.

---

669 See G. Vaciago, 'Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato' (Giappichelli 2012), 81.

670 See F. Zacchè, "L'acquisizione della posta elettronica nel processo penale", (2013) 4 Processo Penale e Giustizia 103, at 103.

671 See M. Daniele, "La prova digitale nel processo penale", (2011) 66 Rivista di Diritto Processuale 283, 290.

III.III. CRYPTOGRAPHY AND NEW INVESTIGATIVE TOOLS.

One of the main problems of cybercrime legislation is the struggle to keep up with the evolution of digital technology. A normative system that fails to do this may be unable to address new types of cybercrime, due to the principle of legality, which mandates a precise construction of criminal offences (*lex certa)* and prohibits the extensive interpretation of liability (*lex stricta)*.[672] Conversely, no strict principle of legality commands procedural law. Even in the absence of a clear procedural framework regulating the use of new technologies in investigations, law enforcement agencies may be allowed to such use by subsuming new technologies under existing procedural rules, or operating in legal "grey areas". The limits to this are to be found in the rules related to the admissibility of evidence. Furthermore, specific requirements may stem directly from human rights obligations both at the domestic constitutional and the international level.[673] Today's evolving technological panorama presents new investigative possibilities. A suspect's laptop, their smartphone, or their smart home appliances store vast amounts of data whose access and collection may be essential for the investigations. At the same time, new technologies may hinder the use of conventional cyber investigation techniques. In particular, cryptography is specifically aimed at shielding communication from access or interception. *Mater artium necessitas*: in the need to access encrypted data, investigation authorities have started to develop and use new investigative tools. In most cases, these measures have begun to be regulated only recently.

III.III.I. CRYPTOGRAPHY: AN INVESTIGATIVE PROBLEM?

With the growing use of digital technologies, communications and data are increasingly exposed to the risk of being unlawfully accessed or intercepted. Probably more than cybercrime, well documented leaks of massively far-reaching State surveillance have raised the awareness of the

---

672 See *supra* § I.II.I. and generally II. See also C. Peristeridou, 'The Principle of Legality', in J. Keiler and D. Roef (Eds), *Comparative Concepts of Criminal Law* (Intersentia 2016), 35

673 See, e.g., ITA, *Costituzione*, Art. 14 and 15. See also *supra* § II.II.IV.

inherent vulnerability of data and digital interaction.[674] The need for privacy in ICT, and security in commercial or private information moving through the Internet, may be met by the use of cryptographic techniques. Data can be disguised using an encryption key and become incomprehensible to anyone who is not in its possession (encryption). The same key can decipher them, restoring the information to its original shape (decryption).[675]

Due to its efficacy and inexpensive cost, cryptography is now widely implemented. Keeping communications and data safe from from external interference has also acquired a substantial commercial value, and encryption has become commonplace in most software and hardware products.[676]

However, cryptography does not only prevent malicious or abusive interference with data. Criminals may exploit this technology and apply it to data that could be useful for the process of criminal adjudication, thereby hindering investigations.

The problems related to cryptography as a barrier to investigation date back to the 1990s, when the private sector started to employ encryption technologies. The attempt of the US Government to restrict users' access to uncompromised encryption of data, in favour of a greater capacity to carry out lawful surveillance, has led to a conflict between the US Government, tech companies, and digital rights groups – the so-called "Crypto-Wars".[677] The US Government demanded either the use of a "key escrow" system – where a cryptographic key is entrusted to the government or a third party, and used when necessary[678] (a sort of *passepartout*) – or a limit to the strength of encryption technologies exported from the US.[679]

This ongoing debate was recently fuelled by problems around the availability of private smartphone data to governmental investigative authorities (see, *inter alia*, the famous FBI v.

---

674 See See B. Whitfield Diffie and S. Landau, *Privacy on the line: the politics of wiretapping and encryption* (n 666), 2-4.

675 *Id.,* 12-13.

676 See e.g. Whatsapp, "Security" <https://www.whatsapp.com/security/>.

677 See D. Kehl, A. Wilson and K. Bankston, *Doomed to repeat history? Lessons from the Crypto Wars of the 1990s* (Open technology institute, 2015).

678 See H. Abelson *et al*, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (Columbia University Academic Commons, 1997).

679 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (2017), 18 ff; D. Kehl, A. Wilson and K. Bankston, *Doomed to repeat history? Lessons from the Crypto Wars of the 1990s* (n 677). Interestingly, the creator of an encryption software released on the Internet was the object of a federal investigation into whether he was illegally exporting cryptographic software (which was at the time considered ammunition) without a license. See K. Finklea, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations* (Congressional Research Service 2016), 3; R. J Stay, 'Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann', (1996) 13 Georgia State University Law Review 581.

Apple case[680] – although similar cases are commonplace) and around the diffusion of encryption technologies in many communication applications, such as WhatsApp[681]. Cryptography therefore remains a significant barrier to criminal investigations.[682]

Leading international figures have supported a "backdoor"[683] approach by pushing for tech companies to intentionally build vulnerabilities into their software. A backdoor provides a route by which investigating authorities can acquire data stored on personal devices.[684] On the other hand, a stable international consensus has backed strong encryption technologies in order to offer robust security to online users.[685] As stated in 2015 by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: "States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows".[686]

Indeed, encryption is a powerful tool to protect data. In the absence of rigid limits to abusive State action, and effective prevention and repression of cybercrime, it appears the simplest solution to privacy issues in digital communications.

Cryptography and investigative solutions.

When data are encrypted, investigators cannot access their content. In the absence of a system of backdoors or key escrows (or weak cryptographic standards), there are two possible solutions for overcoming this obstacle: the introduction in the legal system of an order to decrypt data,

---

680 See D. Yadron, S. Ackerman and S. Thielman, 'Inside the FBI's encryption battle with Apple' (The Guardian, 18 February 2016) <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>.

681 UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 19.

682 See James B Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (FBI, 16 October 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

683 A backdoor is a method to access a computer system bypassing its ordinary authentication and security measures. A backdoor may be created by a developer, so that an application or a system can be accessed for various purposes (such as troubleshooting).

684 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 20.

685 See also Europol and European Union Agency for Cybersecurity, *Joint Statement - On lawful criminal investigation that respects 21st Century data protection*, 20 May 2016, <https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0>.

686 UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 22 May 2015, A/HRC/29/32.

paired with a criminal offence of refusing to decrypt them; and the use of hacking techniques to access systems before decryption.

The first option appears to be the most natural solution, at least technically: compelling suspects or companies that offer built-in encryption technologies in their services to provide the password to decrypt data.

However, when addressed to a suspect/accused, such orders may conflict with the privilege against self-incrimination (*nemo tenetur contra se detegere)*[687]. According to that privilege, evidence cannot be obtained by the suspect/accused against his/her will. In the international system, this privilege is mainly encapsulated in Article 14(3) (g) of the ICCPR, and Article 6 of the ECHR.[688]

In Saunders v United Kingdom, a case related to an obligation to testify imposed by law under a threat of sanction, the European Court of Human Rights stated that "the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seeks to prove its case against the accused without resort to evidence obtained through methods of coercion or oppression, in defiance of the will of the accused"[689].

Of course, the privilege is not absolute, and important exceptions are accepted. ECtHR case-law sketches a test for establishing whether Article 6 permits the use of coercion to obtain information from suspects. The test takes into consideration: the nature and degree of the compulsion used to obtain the evidence; the existence of any relevant safeguards in the procedure; and the use to which any material so obtained is put.[690] As a general rule, the conflict of any compulsion to extract evidence with the privilege against self-incrimination is directly related to two elements. Firstly, the degree of the intellectual effort requested from the suspect/ accused against his/her will. Secondly, the importance of the evidence to be obtained in relation

---

687 Interestingly, this Latin maxim has many different versions (*nemo tenetur… contra se edere, se ipsum accusare, se ipsum prodere…*).

688 See also, in the EU, *Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings*, OJ L 65, 11.3.2016, Article 7

689 ECtHR, *Saunders v. United Kingdom* (Application n. 19187/91), 17 December 1996, § 68.

690 ECtHR, *Jalloh v. Germany* (Application n. 54810/00), 11 July 2006, §117.

to the overall probative architecture of the case.[691] Particular attention should be paid where direct compulsion, such as the risk of a sanction, is involved. However, the risk of infringement is inversely proportional to the preciseness of the information required.[692]

Any analysis of the use of decryption orders in light of the *nemo tenetur* principle may not always lead to a standard outcome. Infringement of this procedural right may depend on several factors, such as the value of the evidence to be decrypted or the level of coercion employed (including accompanying sanctions for refusal).

In framing the scope of the privilege against self-incrimination, the existence of laws that impose ordinary civil obligations is admitted, such as the obligation to inform the police of one's identity[693] or to declare income to the tax authorities[694]. Furthermore, certain human activities may entail specific disclosure obligations, which are inherently related to the nature of such activity (e.g. inform the authorities of the driver's identity in the commission of road-traffic offences)[695], and necessary to balance their potential harm to pivotal societal interests such as public order. If the diffusion of encryption in digital communications will be considered as imposing insurmountable limits to the prevention and repression of crime, the weight of the public interest in maintaining order may crystallise the idea that using encrypted data requires disclosure of keys, without encompassing any infringement on the privilege against self-incrimination.

Instead, when the order to decrypt is addressed to a company, its compliance may lead either to a breach of the contractual terms of the service offered or, at least, to a significant loss of commercial reputation. The protection of customers' data is of pivotal importance to companies. Being obliged to decrypt data or to surrender encryption keys may result in a substantial decrease in commercial trust and competitiveness. For instance, in the United States, two companies preferred to shut down their services instead of complying with decryption orders.[696]

---

[691] See B. J. Koops, 'Commanding decryption and the privilege against self-incrimination', in C. M. Breur, M. M. Kommer, J. F. Nijboer and J. M. Reijntjes (eds), *New trends in criminal investigation and evidence, Volume II* (Intersentia 2000); D. Vitkauskas and G. Dikov, 'Protecting the right to a fair trial under the European Convention on Human Rights', *Council of Europe human rights handbooks* (2012), 63-65; ECtHR, *O'Halloran and Francis v. United Kingdom* (Application n. 15809/02 and 25624/02), 29 June 2007, §§57-62. See also ECtHR, *Saunders v United Kingdom* (n 689); ECtHR, *Gäfgen v. Germany* (Application n. 22978/05), 1 June 2010.

[692] ECtHR, *O'Halloran and Francis v. United Kingdom* (n 691), §57, 58.

[693] ECtHR, *Vasileva v. Denmark* (Application n. 52792/99), 25 September 2003, §32-43.

[694] ECtHR, *Allen v. the United Kingdom* (Application n. 25424/09), 12 July 2013.

[695] ECtHR, *O'Halloran and Francis v. United Kingdom* (n 691), § 57.

[696] See J. Ribero, 'After Lavabit, Silent Circle also shuts down its encrypted email service' (PCWorld, 9 August 2013) <https://www.pcworld.com/article/2046264/after-lavabit-silent-circle-also-shuts-down-email-service.html>.

In Europe, some States have introduced decryption orders. In France, Article 30 of the *Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* allows investigating authorities to order any person to decrypt or surrender encryption keys related to any information encountered during investigations. Failure to comply is punished with imprisonment up to five years, and a fine. In the UK, the Regulation of Investigatory Powers Act 2000 requires persons to decrypt information or surrender keys. Failure to comply may result in a maximum penalty of two years of imprisonment (five, in cases related to national security or child pornography).[697] While Belgian and Dutch systems also envisage orders to decrypt, they can only be administered to system operators or ITCs.[698]

Hacking techniques.

In the last decade, several States have started to employ hacking techniques to remotely access data stored in devices and intercept digital communication passing through them. The reasons why States are employing such methods relate mainly to cryptography. Modern hacking techniques allow access to data at the source, before it is encrypted, and may also disclose passwords used to encrypt data. However, directly accessing data contained in a device or flowing through it is a powerful investigational tool. Its investigative benefits go far beyond cryptography. In particular, this tool may be useful in fighting serious crimes, especially in cases in which criminal groups use new technology to communicate.[699] Indeed, several provisions regulating investigative hacking have been contained in statutes aimed at strengthening the fight against organised crime and terrorism.[700]

In Europe, some States have recently enacted specific provisions regulating the use of hacking techniques. In the UK, such techniques are regulated by the 2016 Investigatory Powers Act, which permits law enforcement to "interfere" with electronic equipment – such as a laptop or a

---

697 As noted by Koops, the measure's invasiveness is balanced by the existence of a system of check and balances and by the court's possibility to exclude compelled evidence (B. J. Koops, 'Commanding decryption and the privilege against self-incrimination' (n 691), 181).

698 NL, *Wetboek van Strafvordering*, Article 125k; Belgium, *Loi du 28 novembre 2000 relative à la criminalité informatique*, Article 9.

699 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 46.

700 See e.g. FR, *Loi n° 2016-731 du 3 juin 2016*. Unfortunately, it is a constant trait of the modern and contemporary legislative theory that the fight against terrorism "justifies" an unbalanced compression of the human rights of the suspect/accused, in favour of the public interest in preventing and repressing the criminal phenomenon.

smartphone – to obtain stored data.[701] The Act also created an Investigatory Powers Commission which, together with the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal, oversees the use of investigatory powers.[702] Likewise, the "*Loi n°2016-731 du 3 juin 2016*" inserted in the French Criminal Procedure Code provisions regulating the "*captation de données informatiques*" (interception of data).[703] Other States still continue to use of hacking techniques without any legal basis, or forcing extensive interpretation of existing provisions. As an example, in Italy – notwithstanding the enactment of specific provisions on data interception through the use of hacking tools[704] – their use to search devices and seize data is still unregulated, and generally based on traditional search and seizure provisions.[705]

Law enforcement agencies have employed hacking techniques for many years. In the majority of cases, hacking has been conducted in the absence of any precise legal basis, forcing a broad interpretation of existing provisions. The FBI has deployed packet sniffers (i.e. software that can intercept and capture traffic that passes over a network) to monitor a target user's Internet traffic since the 1990s'.[706] In 2001, the use by the FBI of a "Trojan horse" (i.e. a program that appears benign but is designed to control or to provide a backdoor entrance to a system) malware aimed at recording keystrokes was reported for the first time.[707]

In Europe, the use by German law enforcement agencies of Trojan horses dates back to 2007. Allegedly, these programs were used to intercept digital communications.[708] The Chaos Computer Club, a digital activist group, analysed the software. Their findings showed that the

---

701 UK, *Investigatory Powers Bill: Equipment Interference,* <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530554/Equipment_Interference_Factsheet.pdf>.

702 UK, Home Office, *Factsheet – Oversight: Investigatory Power Bill* (2015), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473741/Factsheet-Oversight.pdf>; UK, Home Office, Factsheet – *Investigatory Powers Commission", Investigatory Power Bill* (2015), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473744/Factsheet-Investigatory_Powers_Commission.pdf>.

703 See C. Guerrier, "La révision du code de procédure pénale de 2016: le nouveau régime des interceptions électroniques", (2016) Juriscom.net: droit des technologies de l'information .

704 ITA, *Decreto legislativo n° 216 del 29.12.2017.*

705 Inter alia, ITA, Corte di Cassazione, *Judgement n. 16556/09*. See also J. J. Oerlemans, 'Hacking without a legal basis' (Leiden Law Blog, 30 October 2014) <http://leidenlawblog.nl/articles/hacking-without-a-legal-basis>.

706 See Pam Dixon (ed), *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (ABC Clio 2016), 58ff.

707 See B. Sullivan, 'FBI Software Cracks Encryption Wall', (NBS News, 20 November 2001) <http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.WdOKTUyB1mA>; See R. S. Martin, 'Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome', (2003) 40 American Criminal Law Review 1271; C. Woo and M. So, 'The case for Magic Lantern: September 11 Highlights. A need for increased surveillance', (2002) 15 Harvard Journal of Law & Technology 521.

708 See M. A. Gregory and D. Glance (Eds), *Security and the Networked Society* (Springer 2013), 55.

Trojan was also able to perform other investigative actions, such as recording keystrokes and activating webcams.[709]

Various hacking techniques may be employed:[710] law enforcement agencies may exploit systems' vulnerabilities to obtain access to those systems; intruding upon them using false identities; operating brute force attacks (i.e. using software to try all possible passwords and passphrases until the correct one is found); or infect the system with a malware (e.g. a Trojan).[711] Once inside the system, various activities can be carried out: search and seizure of stored data; data alteration; real-time interception of data; capture and recording of the keystrokes on a keyboard; access to the audio/video peripherals of devices and their activation.[712]

Hacking techniques permit retrieval of data stored in a device, interception of passwords and digital/oral communication, and the operation of video and audio functions on a device for surveillance purposes. A purely analogous consideration of the activities allowed by such techniques in relation to conventional investigative categories is reductive. Hacking into a device is more than a mere sum of traditional digital investigation methods. Such activity presents possibilities of unprecedented investigative results, eclipsing traditional cyber investigation techniques. Hacking permits complete and surreptitious access to a device, its content and its external communication, and turns it into a 24/7 live recorder.

At the same time, hacking techniques generate various technical risks and may lead to extreme compression of the privacy rights of an individual.

The use of hacking techniques may weaken the security of the targeted device and, more generally, of the ICT system. Design and implementation flaws in the software used to hack the device may allow others to take control of its functionality, thus significantly compromising the

---

[709] See 'Chaos Computer Club analyzes government malware' (CCC, 8 October 2011) <https://ccc.de/en/updates/2011/staatstrojaner>.

[710] For an in-depth analysis of the use of hacking techniques by investigating authorities in the European Area, see UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679).

[711] *Ibid.*

[712] See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 58ff.

device.[713] Furthermore, the reported use of zero-days vulnerabilities[714] to hack systems is related to a series of issues.[715] It may obstruct patching, as the vulnerability discovered is not reported to the vendor (and thus is not rectified). Instead, it is used to access the targeted system. Stockpiling vulnerabilities leads to risks of their theft and their subsequent use by malicious hackers. To give an example, the famous "Wannacry" ransomware was based on a zero-days exploit stocked by the NSA. In the aftermath of the attack, Microsoft strongly criticised NSA's practice of stockpiling vulnerabilities. Microsoft's President declared that "[we] have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage."[716]

The engagement of law enforcement agencies in black-market trades of vulnerabilities with "black hat hackers"[717], without any oversight or control, can be easily perceived as morally (and possibly legally) reproachable. Moreover, such policies incentivise these black-markets.[718] To this regard, the US system implements a "Vulnerability Equity Process", in which a board scrutinises

---

[713] See 'Chaos Computer Club analyzes government malware' (n 709). Some legislative provisions – such as the German one – require removal of the software used from the target device at the end of the operation. Of particular importance and innovative aim, an Italian draft law, decayed, (ITA, *Proposta di Legge "Quintarelli", Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali*, <http://www.civicieinnovatori.it/wp-content/uploads/2017/02/PDL-Captatori-Legali_DEFV3.pdf>) stipulated that software's production and use must be traceable through a National Registry, which would contain a copy of the software. Moreover, its compliance with the law and technical regulations must be certified, and a specific authority would conserve its source code.

[714] A vulnerability window is a time between the discovery of the vulnerability and the development and publication of a countermeasure to that threat. Zero-day attacks indicate attacks that exploit vulnerabilities previously unknown.

[715] See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 25; S. M. Bellovin, M. Blaze, S. Clark and S. Landau, 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet', (2013) 12 Northwestern Journal of Technology and Intellectual Property 1.

[716] See B. Smith, 'The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack' (Microsoft, 14 May 2017) <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#lEGOIgXOx20j4QgA.99>.

[717] Another element of classification of the computer underground is the ethical framework followed by hackers. A fundamental distinction is made between hackers following a self-regulating ethical code ("ethical hackers"), and those who perform cyber actions outside these ethical boundaries, usually against the law and for personal gain. This distinction classifies hackers according to the colours of an imaginary hacker's hat: white hat hackers (ethical), black hat hackers (criminal), leaving in the middle a vague shade of grey. On the "dark" side lies the cybercriminal, which uses computer technology outside any ethical framework exclusively for personal gain or pure malice. White hats (also called "ethical hackers"), on the other hand, follow a rigid system of ethical principles, and are usually employed in companies as "penetration testers"; while grey hat hackers may follow their own ethical system, operate for the good of society, but still commit illegal acts (thus, also "hacktivists" may fall in that category). Besides ethics, the difference between the three colours may thus be related to the legality of the act. See G. Kirwan and A. Powe, *Cybercrime: The Psychology of Online Offenders* (CUP 2013), 54; P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (Elsevier 2013); R. Moore, *Cybercrime: Investigating High-Technology Computer Crime* (Rutledge 2010), 24-25.

[718] See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 25.

the opportunity to disclose and use a vulnerability for law enforcement purposes.[719] This oversight authority is undoubtedly a virtuous solution to the excessive use and stockpiling of vulnerabilities. No similar processes are envisaged elsewhere.

The use of remote hacking techniques by investigative authorities may also generate problems related to territorial sovereignty in cases where the location of the targeted device is unknown.[720] As will be considered in the chapter on jurisdiction and international cooperation, the nature of the Internet and of the services therein provided may engender a "loss of knowledge of location"[721]. A State's authority may ignore the location of data and devices before conducting the operation. This situation leads to concrete risks of operations targeting data and devices residing outside the State's jurisdiction.[722]

Besides the various technical risks indicated above, the main problematic issue of investigative hacking, and one of the strongest objections to its use (at least, not under strict limitations), is the possible breach to the privacy of the persons involved. The use of hacking techniques is extremely invasive in the private life of the individual. Hacking techniques allow direct access to large amounts of personal data stored in devices and to communications passing through them. It is therefore difficult to reconcile such activity with the right to privacy.[723]

The use of hacking techniques is the most obvious example of the main problem of cyber investigations – the troubling questions that arise around the right to privacy. Increasing amounts of personal information are "digitalised" as technology evolves.

On the one hand, accessing such information is undoubtedly crucial for the process of adjudication. On the other hand, the owner of the relevant data must be protected against

---

719 Leaked document available at: Electronic Frontier Foundation, 'Vulnerabilities Equities Process' (EFF, 2016) <https://www.eff.org/it/document/vulnerabilities-equities-process-january-2016)>.

720 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 28

721 See B. J. Koops and M. Goodwin, 'Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law' (Tilburg Institute for Law, Technology, and Society and Center for Transboundary Legal Development 2014), 42.

722 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 9, 29.

723 See, inter alia, Liberty, *Liberty's response to the Home Office consultation on the Equipment Interference Code of Practice* (March 2015), <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20response%20to%20the%20Home%20Office%20consultation%20on%20the%20Equipment%20Interference%20Code%20of%20Practice%20%28Mar%202015%29.pdf>; Necessary & Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), available at https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf; UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 24.

excessive interference by the State in his/her personal digital spaces, which are increasingly essential in his/her personal and professional life.

III.IV. CYBER INVESTIGATIONS AND PRIVACY RIGHTS.

Collecting information to be used in a criminal trial often requires curtailing the fundamental rights of suspects in the name of public interest in prosecuting crime. Investigative activities are instrumental in the process of criminal adjudication. Nevertheless, they actively interfere with the private sphere of the individual.

The balance between the State's jurisdiction to adjudicate and the individual rights of the persons involved in the process of adjudication is traditionally sedimented in a legal framework indicating the conditions and the modalities of investigative operation. The digital revolution altered this balance, thereby generating significant risks to the privacy of the individual. Furthermore, it modified the very boundaries of the concept of privacy.

However, the exact extent of the change that has taken place is not easy to understand. The difficulties lie partly on the elusive nature of the right to privacy, partly on the constant evolution of technology, and partly on the social changes which have taken place around digital technology.[724]

Early outlining of the concept of privacy came from American legal doctrine, in response to increasing concerns related to the emergence of printing technologies.[725] Control of the circulation of private information was considered essential to maintaining social relationships and personal freedom.[726]

Privacy has two fundamental aspects: the power to keep secret certain information in the private sphere; and the power to control the public use of that information, including when (if at all) it is made public. Traditionally, this right covers private life, family life, communications, and home. The right to privacy protects data about oneself, direct expressions of one's thinking or ego, social expressions, and the physical space in which this information is contained or expressed. The right to privacy also entails the power to dominate the context in which a person acts and expresses his/her intimate life.

---

[724] Privacy is a dynamic process "bound to cultural, political, economic and technological changes." See H. Blatterer, P. Johnson and M. R. Markus, *Modern Privacy Shifting Boundaries, New Forms* (Palgrave MacMillian 2010), 1.

[725] See S. Warren and L. Brandeis, "The Right to Privacy", (1890) 4 Harvard Law Review 193.

[726] See A. R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Mass Market 1971), 25.

However, beyond a core definition, the juridical concept of privacy is difficult to define universally. It continually changes in relation to social and technological evolution.[727] Moreover – to a certain extent – privacy retains a subjective element. Different conceptions can be held on the amount of personal information that a person could accept going public,[728] and such conceptions vary greatly according to time and social context.

Nowadays, the amount of personal data whose privacy needs protection is immensely higher than when traditional investigative tools were conceived. In those early days, private information and communications were mainly held at home or shared through the post. Nor is today's context comparable with the first or second stages of the Internet (the so-called web 1.0 and 2.0). According to the Whatsapp company, in 2017 roughly 55 billion messages, 4.5 billion photos, and 1 billion videos were sent daily via the application.[729] A smartphone may contain more personal information about its owner than any other physical place. Increasingly, accessing someone's device may generate a precise image of a person's private and social life, thereby revealing information about their financial and health, their political views, their frequent movements, their communications, and their social connections.

The personal sphere where the person expresses their private life, and enjoys a privacy expectation, is no longer exclusive to the physical domicile. Most of someone's daily expressions, and most information about them, are formed in their "digital domicile".

III.IV.I.THE CONFLICT BETWEEN PRIVACY AND CRIMINAL INVESTIGATIONS.

The right to privacy finds its prototype in the fourth amendment to the Constitution of the United States. Importantly, here the right is framed in direct relation to the power of the State to adjudicate, as a right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". The right was then inserted in the Universal Declaration of Human Rights, at Article 12 (as a right to protection against general arbitrary interference

---

[727] On the difficulties related to defining privacy, see D. Feldman, 'Secrecy, dignity, or autonomy? Views of privacy as a civil liberty', 47 Current Legal Problems 41; J. J. Thomson, "The right to privacy", (1975) Philosophy and public affairs 295.

[728] Let's take, for instance, the text of the Fourth Amendment to the US Constitution, which frame the overall scope of privacy as everything about a person on which he/she has a "reasonable expectation" it will remain private.

[729] 'Connecting One Billion Users Every Day' (WhatsApp Blog, 26 July 2017), <https://blog.whatsapp.com/10000631/Connecting-One-Billion-Users-Every-Day>.

with their "privacy, family, home or correspondence"), and in the International Covenant on Civil and Political Rights, at Article 17. From such legislation derived Article 8 of the European Convention on Human Rights and, subsequently, Article 7 of the Charter of Fundamental Rights of the European Union, both envisaging a privacy right of the individual.

The right to privacy is a qualified right, and the State power can limit it only under certain conditions. The full enjoyment of the right is thus the rule, and any limitation to it should be considered as a qualified exception ("There shall be no interference by a public authority with the exercise of this right except such as"[730]…).

According to the ECHR and its case law, any limitation to the right to respect for one's private and family life, home and correspondence must be, first and foremost, prescribed by law (principle of legality). Any restriction by a public authority must, therefore, have a legal basis. In Khan v. the United Kingdom[731], for instance, the European Court of Human Rights recognised a breach of Article 8 in the use of covert listening devices which, being merely regulated by guidelines of a ministerial department, was lacking a legal basis.

As protection against arbitrary interference, the law limiting the right to privacy must be sufficiently precise to allow for the foreseeability of the consequence of a given action (foreseeability principle).[732] The degree of precision required varies according to different subject-matters. In general, the precision must be proportional to the seriousness of interference. For instance, the Court recognised that the interception of communication, targeting exceptionally susceptible areas of the private life of the individual, should be handled with particularly precise legislation, to avoid abusive use of such investigation tools. In the Kruslin case[733], the Court held that "tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise." Furthermore, it recognised that detailed rules on such matters were essential to shield the privacy of the individual from the sophistication of the technology used to intercept communication.[734] In the case of Prado

---

730 ECHR, Article 8.

731 ECtHR, *Khan v. the United Kingdom* (Application n. 35394/97), 12 May 2000. See also UN GA, Human Rights Committee, *General Comment N. 34 (Article 19 ICCPR)*, 12 September 2011, § 25.

732 See, inter alia, ECtHR, *Andersson v. Sweden* (Application n. 20022/92), 25 February 1992, § 75.

733 ECtHR, *Kruslin v. France* (Application n. 11801/85), 24 April 1990.

734 However, in the Malone case (ECtHR, *Malone v. the United Kingdom* (Application N. 8691/79), 2 August 1984) it also recognised that foreseeability requirements "cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly".

Bugallo v. Spain relating to surveillance measures, the Court listed a series of normative requirements, indicating that the law should specify "[the] nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration [of telephone tapping]; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed"[735]. In the Weber & Saravia case, the Court presented a series of minimum safeguards to be set out in the relevant statute law to avoid abuses of surveillance: "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to [be intercepted] (…); a limit on the duration of [the interception] (…); the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed".[736]

Moreover, any compression of privacy rights should be necessary for pursuing a legitimate aim (principle of legitimate purpose). Art. 8(2) ECHR contains a list of potential legitimate purposes large enough to cover most government activities.[737] Crime prevention and protection of national security are among them.[738]

The final requirement is related to the principle of necessity and proportionality. The interference must be necessary and proportionate, that is it "corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"[739]. This requirement includes – inter alia – the various procedural safeguards related to the application of any investigative measures, which must be calibrated on the type and intensity of the interference. With regards to surveillance, the ECtHR has laid down a test which "depends on all the circumstances of the case, such as the nature, scope and duration of the possible

---

[735] ECtHR, *Prado Bugallo v. Spain* (Application N. 58496/00), 18 February 2003, § 30. See also ECtHR, *Roman Zakharov v. Russia* (Application n. 47143/06), 4 December 2015 (Grand Chamber).

[736] ECtHR, *Weber & Saravia v. Germany* (Application no. 54934/00), 29 June 2006, § 95.

[737] See W. Shabas, *The European Convention on Human Rights* (OUP 2015), 404.

[738] In 2106, in the Szabò & Vissy case (ECtHR, *Szabó and Vissy v. Hungary* (Application no. 37138/14), 12 January 2016), on the "potential of cutting-edge surveillance technologies to invade citizens' privacy", the Court noted that "a measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (…) – an approach it considers convenient to endorse."

[739] ECtHR, *Olsson v. Sweden* (Application n. 10465/83), 24 March 1988.

measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures and the kind of remedy provided by the national law".[740]

The principle of proportionality is one of the most critical elements of the right to privacy, since it regulates the balance between privacy and the State's interests. As stated in Soering v. UK, "inherent in the whole of the Convention is a search for a fair balance between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights".[741] With regards to criminal law, the principle of proportionality is increasingly detached from a flat bilateral weighing of the public and private interest, and more oriented towards a human rights-based approach, as an exception to the presumption of innocence and a derogation of the rights of the accused.[742] In evaluating such an exception, the independent authority overseeing an investigation (often a magistrate) plays an essential role. That authority is required to consider whether such derogation is justified. As stated by the ECtHR in Letellier v. France: "national authorities must examine all the circumstances capable of proving or disproving the existence of a genuine public interest, justifying an exception to the general rule that individual liberty must be respected, bearing in mind the presumption of innocence."[743]

The other international instruments envisaging the right to privacy encompass similar tests. For instance, Article 17 ICCPR requires that any restriction is provided by the law, is necessary for reaching a legitimate aim, serves one of the enumerated legitimate aims, and conforms to the principle of proportionality (i.e. the measures taken are appropriate to achieving their purpose, being the least intrusive instrument available and proportionate to the interest protected by its use).[744]

However, no international instrument pays specific consideration to the newest digital tools of investigation.

ICT technology and their challenges to privacy rights are mainly considered with regards to breaches related to data processing by private entities. Although not focused on criminal

---

[740] ECtHR, *Klass and others v. Germany*, (Application n. 5029/71), 6 September 1978, § 50.

[741] See ECtHR, *Soering v. the United Kingdom* ((Application n. 14038/88), 7 July 1989. See also R. C.A. White and C. Ovey, *The European convention on human rights* (OUP 2010), 308ff.

[742] See M. Delmas Marty and J. R Spencer, *European Criminal Procedures* (CUP 2006), at 532.

[743] ECtHR, *Letellier v. France* (Application n. 12369/86), 26 June 1991, § 35.

[744] UN GA, Human Rights Council, *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40.

investigations, this normative framework may provide "external" limitations to cyber investigations.

In the 1970s, the pressure exerted by technological evolution on privacy rights led to the adoption, under the aegis of the Council of Europe, of a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[745] The Convention is the first binding international instrument to protect the individual from abusive collection and processing of personal data and to regulate their transnational flow. It limits the processing of "sensitive" data (such as data on a person's race, politics, health, religion, sexual life, or criminal records). Furthermore, it recognises the individual's right to know about the existence of information stored on them, and possibly to have it corrected.

The CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was used as a basis for Article 286 EC, the General Data Protection Directive 95/46/EC[746], and Article 8 of the European Charter on Fundamental Rights. In particular, Article 8 of the European Charter expressly addresses the protection of personal data.

From a European human rights perspective, Privacy in ICT is regulated by both the provisions of the ECHR and ECFR, and the "secondary" laws on data protection. Of particular importance are a series of EU instruments governing the retention and processing of personal data by the public and private sector.[747] Three EU instruments regulate personal data retention: Directive 95/46/EC, Directive 02/58/EC, Regulation (EU) 2016/679 – repealing Directive 95/46/EC – and Directive 2006/24/EC. The latter was however invalidated by the ECJ in the famous case Digital Rights Ireland[748]. A Council Framework Decision (2008/977/JHA of 27 November 2008) regulates the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Directive 2016/680 of 27 April 2016, aimed at repealing Council Framework Decision 2008/977/JHA, focuses more broadly on the protection

---

745 See S. Peers, T. Hervey, J. Kenner and A. Ward, *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014), 228.

746 Which was followed by other legislative acts on the topic, as indicated *infra*, in particular by EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.*

747 Data protection provisions are also envisaged in the EU primary law: Article 16 of the Treaty on the Functioning of the European Union provides that "everyone has a right for the protection of the data concerning them." Moreover, Article 16(2) of this Treaty mandates the European Parliament and the Council to lay down the rules regulating the protection of natural persons in relation to the processing of personal data and their free movement.

748 See, *inter alia*, F. Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States', (2015) 28 Harvard Human Rights Journal 65; M. P. Granger and K. Irion, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection", (2014) 39 European Law Review 835.

of natural persons with regard to the processing of personal data[749] by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data[750].

Data retention instruments (with particular regard to the EU Regulation 2016/679) lay down rules regulating the processing of data (e.g. collection, storage, use, disclosure or dissemination) and the rights of the data subject. They are tangential to the investigative powers exerted by state authorities. However, they carve the scope of privacy rights obligations, and may directly, and *ex ante*, limit the scope of the State's investigative power. For instance, they can set constraints on the nature and quantity of data controlled and stored by an ITC (and there collectable by the investigative authorities).[751]

EU Directive 2016/680 is the only instrument directly affecting cyber investigations. It regulates the protection of natural persons' privacy with regard to the processing of their personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The framework set forth by the Directive revolves around a series of principles regulating data processing. Data processing should be lawful and fair, and carried out only for specific and legitimate purposes. Data collected should be accurate, adequate to the purpose, not excessive, and not kept longer than necessary. Data subjects are empowered with a series of rights, such as the right to information

---

749 EU, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (n 637), Article 3 – Definitions: "For the purposes of this Directive (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

750 The Directive 2016/680 is thus *lex specialis* in relation to EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (n 746): where such personal data is processed for purposes other than for those of the Directive, Regulation (EU) 2016/679 applies.

751 Although the State may provide restriction to the scope of a series of obligations and rights by way of legislative measure for – inter alia – the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (*Id.*, Article 34 of the EU Regulation 2016/679)

on data processing concerning them, access to and rectification or erasure of personal data,[752] and the right to a remedy where data processing of personal data infringes provisions adopted pursuant to the Directive.

Due to their far-reaching scope, the said instruments – constituting a specification of the privacy rights envisaged in the ECHR and the EU law – function as external limits for cyber investigations. However, the content and application of these instruments leaves unanswered the question of whether the use of cyber investigation tools is compatible with the privacy rights of the suspect or accused.

III.IV.II. PRIVACY AND CYBER INVESTIGATIONS.

From a normative point of view, human rights issues related to law enforcement actions on the private digital space are often ignored. No specific provisions can be found in the human rights instruments, nor in the instrument on cybercrime – notwithstanding significant attention to human rights aspects in the procedural aspect of the Budapest Convention.

Article 15 of the CoE Convention on Cybercrime addresses a series of conditions and safeguards to which the modalities of establishing and implementing its procedural law provisions are subordinated. Such conditions and safeguards are aimed at providing an adequate balance between law, enforcement interests and the protection of human rights.[753] Specifically, the Article requires that the powers and procedures provided for in Section II of the Convention be subject to the conditions and safeguards envisaged domestically, which shall provide for adequate protection of human rights and liberties, including rights arising pursuant to international human rights instruments. The Convention does not specify the nature of these conditions and safeguards. However, it explicitly references the 1950 Council of Europe

---

[752] EU, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (n 637), Preamble § 44: "Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others.".

[753] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 145.

Convention for the Protection of Human Rights and Fundamental Freedoms – although not all Parties to the Convention are party to it – and the 1966 United Nations International Covenant on Civil and Political Rights, plus a general reference to "other applicable international human rights instruments".

Specific direct incorporation of the principle of proportionality is provided by the Convention on Cybercrime, as a definite limit to the powers and procedures thereby envisaged.[754] As previously stated, the principle of proportionality is directly linked to judicial overview. If there is a conflict between the community interest in crime repression and the fundamental rights of the individual, the proportionality principle traditionally mandates that only the minimum necessary compression may be done to the rights of the individual. The principle also limits the excessive use of power to cases where the compression of human rights is "a lesser evil than allowing events to take their course."[755]

As a specification of the proportionality principle, the Budapest Convention stipulates that – based on the applicable domestic law and within a margin of State's discretion – the above-mentioned condition and safeguards should include "judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure". Furthermore, the Convention requires each Party to consider the impact of the investigative powers and procedures upon the rights, responsibilities, and legitimate interests of third parties (such as protection of consumer services from disruption, or of proprietary interests)[756]. These rights, responsibilities, and legitimate interests (and the measures aimed at their protection) should only be considered if they are consistent with the investigative needs or other public interests, such as the fundamental rights of the suspect or the victim.

Human rights limits to the use of cyber investigation tools are mainly found in the traditional privacy framework. A series of soft law instruments reiterate the need for following such rules. Of particular importance is the Third Resolution on the right to privacy in the digital age that was adopted in November 2016 by the UN General Assembly.[757] The Resolution addresses the human rights issues related to surveillance of communications, their interception, and the collection of personal data by State authorities. It affirms that the same rights, including the

---

754 Cfr the UN GA, Human Rights Council, *Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,* A/69/397, 234 September 2014, stating that "proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest" (§ 51).

755 See, *inter alia*, A. Ashworth, *Principles of Criminal Law* (n 433), 57.

756 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 148.

757 UN GA, *Resolution A/RES/71/199 The right to privacy in the digital age*, 25 January 2017.

right to privacy, that people have offline must also be protected online. The Resolution calls upon States: "(t)o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law; to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data; (and) to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations".

Similarly, the 2013 Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[758] proposed the following recommendations to States: "(l)egislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in the law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State (…) and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath. Legal frameworks must ensure that communications surveillance measures: (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application; (b) Are strictly and demonstrably necessary to achieve a legitimate aim; and (c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted."[759]

---

[758] There, the Special Rapporteur recognised that "(p)rivacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other".

[759] See UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, 17 April 2013.

The UN GA Resolution and the Report of the Special Rapporteur substantially reiterate earlier international obligations related to privacy rights.[760] Such reaffirmation appears necessary: as stated by the Special Rapporteur, "national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression."[761]

Privacy and hacking by law enforcement.

Let us return to the hacking tools employed by State investigative authorities, and the various issues related to their clear impact on the human rights (in particular privacy) of the persons involved.

Their use must be, first and foremost, regulated by law. Many systems still lack a precise regulation of their use. This void militates against the above-mentioned principle of legality, mandated by the international human rights instruments and many State constitutions. [762]

Furthermore, the law regulating their use must be sufficiently clear and precise as to consider their versatility (which allow various investigative activities) and indicate acceptable standards of operation.[763] Different functions may require autonomous consideration of necessity and proportionality, as well as separate authorisations. Virtuous examples can be found in a 2016 amendment to the Polish Police Act – which previously generically allowed the use of "technical means" – specifying the activities permitted ("extracting and recording data from data storage media, telecommunications, terminal equipment, information and communication systems").[764]

---

760 Similarly, UN GA, Human Rights Council, *The right to privacy in the digital age*, A/HRC/34/7, 27 February 2017, affirming that "States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality".

761 See UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (n 759), § 3.

762 Such as, for instance, ITA, *Costituzione*, Article 14 and 15. However, the lack of a legal basis for this investigative method has not been yet contested by national or international jurisprudence. For instance, before a normative reform introducing a provision on "hacking", a series of decisions from the Italian Court of Cassation validated such use based on the traditional investigative provisions (ITA, Corte di Cassazione, *Judgments n 24695/2009 and 254865/2012)*.

763 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 58.

764 *Ibid*. Poland, *Police Act (Text No. 179)*, Article 16 § 6.

Likewise, the Dutch Computer Crime III Act lists both the functionalities and the techniques that may be used during hacking by law enforcement.[765]

The principle of necessity and proportionality should govern the use of these new investigative measures. An *ex ante* assessment of the necessity and proportionality of the measure concerning the severity of the infringement on the rights involved must be provided by law.[766] Judicial authorisation[767] is therefore of primary importance, as is limiting the use of hacking techniques to crimes of substantial gravity. In line with the former requirement, the French Criminal Procedure Code requires judicial review, on the request of the public prosecutor, for hacking tools to be used.[768] In the UK, the warrant on the use of hacking tools must be approved by a Judicial Commissioner, an authority that was created *ad hoc* by the Investigatory Power Act. The Judicial Commissioner is required to apply "the same principles as would be applied by a court on application for judicial review".[769] The Investigatory Power Act expressly requires the Commissioner to consider the necessity and proportionality of the warrant.[770] However, many civil rights associations have highly criticised the limited role of such a quasi-judicial overview.[771]

The use of hacking tools should be permitted only with regard to particularly serious offence, according to the principle of proportionality. With this regard, the German system provides – at § 100a(2) *Strafprozessordnung* – a list of serious offences on which the hacking techniques can be applied.[772] In France, the "*captation des données informatiques*" can be employed exclusively in organised crime cases.[773]

---

765 See UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (n 679), 59.

766 See EU, European Data Protection Supervisor, *Dissemination and use of intrusive surveillance technologies, Opinion 8/2015*, 15 December 2015, 10.

767 See also UN GA, Human Rights Committee, *Concluding Observation on the Sixth Periodic Report of Italy,* CCPR/C/ITA/CO/6, 28 March 2017, on "hacking of digital devices", requiring "judicial involvement in the authorization of such measures in all cases".

768 FR, *Code de Procédure Pénale*, Artt. 706-102-1, 706-102-2.

769 UK, *Investigatory Power Act*, § 23(2)a.

770 *Id.*, § 23(1).

771 See Liberty, 'Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Commons' (March 2016), <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20summary%20of%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>.

772 See also Organization of the American States, Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, *Concerns over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere*, Press Release R80/15, 21 July 2015: "according to international standards, the use of programs or systems for the surveillance of private communications should be clearly and precisely established by law, genuinely exceptional and selective, and must be strictly limited to the needs to meet compelling objectives such as the investigation of serious crime as defined in legislation."

773 FR, *Code de Procédure Pénale*, Artt. 706-102-1, 706-102-2.

Other essential conditions may be necessary to reconcile the use of such methods with the right to privacy. Some are related to the appropriateness of the tools used, also from a technical point of view.[774] Due to the evolution of the complexity of techniques used, any evaluation of the necessity and proportionality of proposed hacking measures should be based on the technical details of the measure in question.[775] Some conditions are related to the scope of the measure, limiting it to devices used by the suspect[776], and reducing the duration of the operation to what it is strictly necessary[777]. Others are related to the integrity of data (and their further admissibility as evidence)[778], and the deletion of non-relevant or private data[779]. Finally, considerations relating to the notification of the targeted subject of the existence of hacking operations – at least once surveillance has been completed – and his/her connected right to an effective remedy should be envisaged.[780]

III.IV.III. THE NEED FOR A DIFFERENT APPROACH TO PRIVACY.

As evaluated in the previous sections, the existing hard and soft norms related to cyber investigation merely stress the importance of subsuming such tools under the existing privacy framework. However, several new tools are currently used by law enforcement agencies without the necessary requirement to reconcile them with the right to privacy.

---

774 GER, *Bundeskriminalamtgesetz*, §20k.

775 See Privacy International, *Hacking Safeguards and Legal Commentary*, § 3 Necessity and Proportionality (privacyinternational.org, 11 June 2018) <https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary>.

776 GER, *Strafprozessordnung,* § 100a(3). See, on this point, US, *United States v. Werdene*, No. 16-3588 (3d Cir. 2018), and the other so called "Playpen cases" (C. M. Bell, 'Surveillance Technology and Graymail in Domestic Criminal Prosecutions', (2018) 16 Georgetown Journal of Law & Public Policy 537; S. D. Brown, 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' in (2019) ERA Forum.

777 FR, *Code de Procédure Pénale*, Artt. 706-102-1, 706-102-2.

778 This requirement is linked to the technical aspect of the measure, which may influence data. On this point, see UNODC, *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (UN 2009), 21-25; UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (n 759), § 62, also recognizing the possible breach to procedural fairness rights.

779 GER, *Strafprozessordnung,* § 100a(4); GER, *Bundeskriminalamtgesetz,* § 20k (7). The ECtHR case law has recognized that destruction of personal data as soon as they are no longer needed may reduce the effects of the interference with the privacy rights of the suspect (See e.g. ECtHR, *Weber & Saravia v. Germany* (n 736), § 132).

780 See, e.g., UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs*, Legal Frameworks for Hacking by Law Enforcement* (n 679), 52ff; UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (n 759), § 82.

While hacking techniques have been widely used for over ten years, new technologies are emerging. In recent years, there is a growing use of new investigative tools – such as facial recognition technologies – which at the moment remain entirely unregulated.[781]

New cyber investigation methods may exponentially present new and serious privacy issues. Their use requires particular attention by legislators, which should regulate and limit it under the existing human rights obligations.

In particular, limitations to the indiscriminate use of new technologies shall be derived from the right to privacy of the individual concerned. As of 2019, there are three cases open before the ECtHR, challenging the use of new hacking methods *vis à vis* Article 8 of the European Convention[782] The construction of international case law on the subject will undoubtedly aid the rapprochement between these methods and individual rights.

It is doubtful, however, that the mere subjugation of such techniques to the traditional privacy framework – while highly desirable at this stage – is able to satisfyingly address the problem *per se*.

As stated by the European Data Protection Supervisor, privacy and data protection legislation "might not be sufficiently specific to address all the issues raised by the use of privacy-affecting technologies in the context of investigation and law enforcement"[783]. A change of paradigm might be necessary.

It is imperative to consider how digital tools have changed the concept of privacy, and how much privacy is to be expected in cyberspace. The digital expression of a person's life must be safeguarded by offering protection to digital devices containing private data about them. As advocated by the European Data Protection Supervisor, "the "virtual domicile" should be protected with the same respect as the physical domicile."[784]

---

781 See, e.g., M. Jacob, 'Facial recognition gains grounds in Europe, among big-brother fears' (Euroactive, 20 October 2017 <https://www.euractiv.com/section/data-protection/news/facial-recognition-gains-grounds-in-europe-among-big-brother-fears/>; Interpol, ìFacial Recognition' (Interpol.int), <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition>.

782 Although they focus on intelligence interception. ECtHR, *Privacy International and Others v. The United Kingdom* (Application n. 46259/16), on the UK bulk equipment interference regime; ECtHR, *Association Confraternelle de la Judiciaire v. France* (Application n. 49526/15), on the French security service interceptions, also using IMSI catchers, which can collect mobile phone data and track individuals' locations. ECtHR, *Big Brother Watch and Others v. The United Kingdom* (Applications n. 58170/13, 62322/14 and 24960/15), 13 September 2018 (case referred to the Grand Chamber in February 2019), was on bulk intelligence interception, "following revelations by Edward Snowden relating to the electronic surveillance programmes operated by the intelligence services of the United States of America and the United Kingdom".

783 EU, European Data Protection Supervisor, *Dissemination and use of intrusive surveillance technologies* (n 766), 10.

784 *Id.,* 11.

Such considerations should be made at the constitutional level, recognising new rights that transcend the traditional core of privacy legislation. In this regard, of cardinal example is the path taken by the German jurisprudence.

In 1983, the German Federal Constitutional Court developed the notion of *informationelle selbstbestimmung* (digital self-determination). In the *Volkszählungsurteil*, the Court acknowledged a right to informational self-determination based on the general right of personality as protected by Article 1 (Human Dignity) in conjunction with Article 2 (Right to Liberty) of the German Constitution.[785] This doctrine evolved towards the right of a person to develop their personality online. In a subsequent 2008 ruling about the constitutionality of remote searches of computers by government agencies, the Court recognised a new constitutional "right to confidentiality and integrity of information systems", complementing the "fundamental right to informational self-determination".[786]

The German doctrine follows and perfects the "closed container" approach developed by American case law on privacy in ICT.[787] According to this approach, digital devices are to be considered closed "places" where the individual has a reasonable expectation of privacy. Similar consideration to digital devices can be found in the theories on the "information domicile", developed around the legal good protected by substantive cybercrime norms.[788]

The German Constitutional system provides for a set of rights that consider cyberspace both from the user point of view – as their right to develop their personality online – and from a device point of view. It acknowledges that computer systems should be protected *per se*, in their integrity, as they contain relevant parts of the life and personality of a person.

This privacy-by-device approach is a logical starting point for developing an accurate new set of rights in cyberspace. As stated by the US Supreme Court in United States v. Andrus: "(a) personal computer is often a repository for private information the computer's owner does not intend to share with others. For most people, their computers are their most private spaces."[789]

A final consideration could help to understand why digital domiciles must be stringently protected against breaches by law enforcement agencies.

---

785 GER, Bundesverfassungsgericht, *Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83*.

786 See P. De Hert, 'Identity management of e-ID, privacy and security in Europe. A human rights view', (2008) 13 Information security technical report 71, 75.

787 See, ex plurimis, US, Supreme Court, *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."). See also O. S. Kerr, *Searching and seizing computers and obtaining electronic evidence in criminal investigations* (Office of Legal Education, Executive Office for United States Attorneys 2001).

788 See *infra* § II.III.I.

789 US, Supreme Court, *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007)

In the face of justice, no fundamental liberty is absolute. A criminal trial is a place where the liberties of the suspect and the accused are reduced to varying degrees in the name of the efficiency of justice. This efficiency is the reason justifying the use of powers that invade the juridical sphere of the private citizen. The strict connection between the compression of liberty rights and the trial mandates the commensuration of the investigation instruments with the aim of the adjudication process, which is to reconstruct a historical fact. Investigations cannot be used for indiscriminately searching for information on the commission of other crimes (s.c. fishing expeditions), or for social and criminal control.[790]

The relation between the criminal trial and privacy (as in the case of the other liberty rights of the individual) is a relation exception to rule. The functional compression of privacy within the scope of the trial, and in light of the principle of innocence, must therefore leave this right to be able to re-expand to its original limit, once the functional necessity to curtail it ceases to exist.

Today, investigative authorities possess tools that can subjugate an individual to total control by the State. Having full command of the content of and the communications passing through a smartphone, or controlling the identity of the passers-by with face-recognizing cameras, creates the risk of utterly erasing the very idea of privacy.

The possibility of collecting limitless information on a suspect will lead to an Orwellian level of control. Indeed, 1984's television was frightfully similar to a "trojan" inside a smartphone or a smart home appliance, such as Amazon's Alexa or Google Home. Excessive use of digital technology by law enforcement agencies is to be feared. It may lead to a totally transparent society, where criminal repression will become social control.

As privacy is a subjective concept, juridical evolution must necessarily pass through social evolution. It is therefore imperative to fully appreciate the intimate anthropological value of data and cyberspace and to protect them from external intrusions.

The more laws and behaviours limiting privacy are silently accepted, the less “expectation” of privacy will exist.

---

[790] This delicate balancing between liberty rights and public interest to crime prevention find its natural place in the criminal trial, and in its procedural norms, which should encompass adequate protection of human rights (also due to their inferior hierarchical rank). Any compression to privacy extended outside the criminal trial will – first and foremost – subtract it to the control of the judicial authority which, pondering on the specific need of the trial, must evaluate if the use of investigative powers may indeed lead to a positive outcome for the trial, proportionating such use to the concrete exigencies at stake.

IV JURISDICTION AND INTERNATIONAL COOPERATION

A butterfly taps its keyboard in New York and produces a hurricane in China[791]

[791] A digital version of the so-called "butterfly effect"?

IV.I. INTRODUCTION

Cybercrime is a typical transnational offence. Obviously, it is not the only type of crime whose preparation, commission, or effects may cross borders. Typical transnational crimes are, for instance, those related to cash flow (e.g. money laundering) or illegal traffics (e.g. drug or human trafficking). As such, these crimes require strict cooperation between the relevant States and a concerted international response.

Cybercrime, however, can be considered the transnational crime *par excellence.* Today, cybercrimes are mostly committed through the Internet. Exploitation of the Internet's "worldwide" structure means cybercrime does "not stop at conventional state-borders"[792]. Cybercrime is the only crime that naturally acquires a transnational feature due to the international nature of an element of the crime.

The first issue to be addressed in order to understand the jurisdictional and cooperation problems in the fight against cybercrime is related to this element. How should "cyberspace" be defined? Is it a common space, a supranational spatial and temporal dimension? Alternatively, is it merely a physical construction made of devices which reside in a specific location and are thus directly subject to a territorial State's jurisdiction?

Besides these metaphysical issues on the nature of cyberspace, international cooperation in the fight against cybercrime is affected by myriad concrete problems. The perpetrators of cybercrimes, the victim(s), or the targeted systems or data, may reside in various countries, and the effect of the crime may spread across different jurisdictions.[793] The application of the traditional principles of jurisdiction may lead to more than one jurisdiction being activated by the same cyber act. Such jurisdictions may conflict and thus create the risk of a *bis in idem.*

The fight against cybercrime requires a recalibration of the principles of jurisdiction, or at least the development of a system to prevent and resolve conflicts in this area.

Furthermore, digital evidence may be scattered across multiple jurisdictions. Gathering all the relevant evidentiary elements for the process of adjudication often demands the use of

---

792 EU, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,* [2000] COM/2000/0890, §1.1.

793 Empirically, most cyber activities involve a transnational element. See e.g. UNODC, *Comprehensive Study on Cybercrime* (n 66), 183 ff.

transnational cooperation mechanisms. In such cases, States may necessitate fast cooperation responses, possibly even through informal cooperation methods. Cyber-specific tools of cooperation may be required to address the characteristics of data. In some cases, the investigative authorities may desire to extraterritorially access data[794] or request assistance directly to private entities controlling data without relying on cumbersome cooperation mechanisms with the territorial State.

The protection of the fundamental rights of the person involved should maintain a central relevance. It is imperative to emphasise the importance of the conventional limits to mutual assistance and to consider new limits to potential human rights violations in cyber-specific cooperation. For instance, the extended spatial reach of a cyber conduct may create the risk of an individual being prosecuted for acts which do not constitute a punishable offence in the State where he/she is acting (e.g. because such acts are there covered by the right to freedom of speech). In such a case, the double criminality principle and the political offence exception to cooperation may be fundamental in avoiding their punishment. Furthermore, new cyber-specific forms of extraterritorial investigative activity – such as transnational access to data or direct cooperation with private entities – are emerging. These forms of not based on the traditional cooperation framework, and do not follow its traditional limits. Particular attention has therefore to be made in reconciling them with the human rights of the persons involved.

[794] At least those publicly accessible, or private data with the consent of their owner.

IV.II. JURISDICTION IN CYBERSPACE: APPLYING TRADITIONAL CONCEPTS TO A VIRTUAL SPACE.

Jurisdiction pertains to the power of a sovereign State to regulate, adjudicate, and enforce its laws.[795] In particular, criminal jurisdiction refers to the range of application of the State's *ius puniendi* over conduct that violates its imperative norms. Rules and principles of jurisdiction regulate this range of application over space, persons involved in the violation of the norms, and interests protected.

Traditionally, jurisdiction is grounded on the principles of state sovereignty, equality of states, and non-interference in domestic affairs,[796] which are reflected in the State's power to apply criminal law over acts that take place in its territory. The principle that regulates the territorial application of jurisdiction – the territoriality principle – represents the primary, uncontested basis on which jurisdiction is exercised.[797] Extraterritorial bases for jurisdiction may simultaneously be provided for in the domestic law of a State and are limited by international law.[798] The main principles upon which extraterritorial jurisdiction may be established are: the principle of active personality (which grounds jurisdiction on the nationality of the suspect/ accused); the principle of passive personality (which grounds jurisdiction on the nationality of the victim); the principle of flag State (which grounds jurisdiction on the nation of registration of the aircraft or ship); the principle of protection (which grounds jurisdiction on the interests

---

795 See, inter alia, UN GA, *United Nations Report of the International Law Commission*, A/61/10, Annex E, 11 August 2016, at 517-518.

796 See, e.g., M. N. Shaw, *International Law* (OUP 2008), 645.

797 See, e.g., CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (1990), 8; UK, *Re Wood Pulp* [1998] 4 C.M.L.R 901 at 920; Permanent Court of International Justice, *S.S. Lotus (France v. Turkey)*, 7.9.1927, SER. A n. 10 "… in all systems of law the principle of the territorial character of criminal law is fundamental…".

798 See, inter alia, *id.* at § 18/19 "Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention. "It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law (...) In these circumstances, all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction within these limits, its title to exercise jurisdiction rests in its sovereignty."

protected by the State and violated by the offence); and the principle of universality (which grounds jurisdiction on the universal interests violated by the offence)[799].

Naturally, cybercrime stretches the scope of the traditional principles of jurisdiction, thereby creating a peculiar accumulation of various laws applicable to the same act and conflicts of jurisdiction. In addition to the uncertainty regarding the applicable law and conflicts between prosecuting States, this situation may generate risks for the suspect/accused to be subjected to multiple prosecutions and multiple judgments on the same facts, in violation of the *ne bis in idem* principle.

Applying traditional principles of jurisdiction on cybercrime seems to be unable to avoid conflicts of jurisdiction. On the contrary, it may lead to stimulating their multiplication. Cybercrimes may touch upon, and activate, various jurisdictions. The offender(s) and the victim(s) may be located in different countries. The crime may spread its effects and touch the interests of various States. Data may pass through numerous territories. In some cases, due to the increasing use of cloud computing, the *locus commissi delicti* may be unclear, or fragmented in multiple jurisdictions[800].

Notwithstanding the spatial characteristics of cybercrime, cybercriminal activities are usually subject to the same jurisdictional principles applicable to any form of criminal conduct.[801] At the level of hard law, no cyber-specific international instrument contains tailored jurisdictional solutions. Typically, such instruments encompass an obligation to establish jurisdiction over the substantive offences therein contained on the basis of traditional jurisdictional principles, with a particular focus on the principle of territoriality.

---

[799] See: M. N. Shaw, *International Law* (n 796), 652 ff.; CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (n 797), 9-16; UN GA, *United Nations Report of the International Law Commission* (n 795), 523-526. The representation principle, according to which jurisdiction is transferred from a State (which has jurisdiction over the act under one of the above-mentioned principles) to another State which is charged to represent it, may indeed be considered a "derivative" principle of jurisdiction.

[800] Since a "cloud" may contain data that are physically distributed among various servers.

[801] See M. N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017), 51.

IV.II.I. THE PRINCIPLES OF JURISDICTION.

Principle of Territoriality.

The State's duty/power to prosecute offences committed in its territories derives from the principle of territorial sovereignty and its corollary duty/power to maintain order therein.[802] The focal element of this jurisdictional ground is the concept of the *locus commissi delicti* (place of commission of the crime). The principle may cover offences committed entirely or partially in the State's territory. It can be expressed according to three different formulations:[803] territorial jurisdiction *stricto sensu*; subjective/objective territorial jurisdiction (or doctrine of ubiquity);[804] and the effect doctrine.[805]

The principle of territoriality *stricto sensu* covers offences committed entirely in the territory of the State. Given the peculiar transnationality of new technology as a means of propagation of a crime, the offender and the victims are often located in different jurisdictions, and the *iter criminis* transcends borders. Thus, this "ordinary" inflexion of the principle may find limited efficacy with regard to cybercrime.

Many States recognise a broader scope to the principle of territoriality.[806] The principle of subjective/objective territoriality (or doctrine of ubiquity)[807] covers offences committed only in part in the territory of the State. This *lato sensu* interpretation of the principle is endorsed in the CoE Convention, which recognises territorial jurisdiction when the sole computer system

---

802 See M. N. Shaw, *International Law* (n 796), 653.

803 The subjective/objective territorial jurisdiction and the effect doctrine are not considered "purely" territorial. since they contain an extraterritorial element.

804 See, inter alia: R. J. Currie and J. Rikhof, *International & Transnational Criminal Law* (Irwin Law 2010), 62-64 (objective: the act starts in one State but finishes in the forum State; subjective: the act begins in the forum State but finishes in a different State).

805 *Id.* 64.

806 See, *inter alia*, ITA, *Codice penale*, Article 6: "Offense is considered to have been committed within the territory of the state when the action or omission giving rise to the offence is carried out wholly or partially there, or if the result of the action or omission took place there"; GER, *Strafgesetzbuch*, §9(2): "An act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or at which the result, which is an element of the offence, occurs or should occur according to the understanding of the perpetrator".

807 See UN GA, *United Nations Report of the International Law Commission* (n 795), 521.

targeted is within the State territory.[808] The specific extension of this principle in domestic systems is often left to judicial interpretation, which defines its limits.

The scope of the principle may even cover offences whose *iter criminis* only passes through the territory (i.e. data only transiting through computer systems or nodes located in the territory).[809] This broader interpretation of the territoriality principle is endorsed, for instance, in Italy.[810] Likewise, the US State of West Virginia penal code extends its jurisdiction over anyone who violates any provision of the State's computer crimes code "and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, *or passes through this state in transit*."[811] Similar provisions can be found in Malaysian and Singaporean jurisdiction clauses.[812] This variant of the principle dramatically extends the scope of application of the territorial jurisdiction, granting it to the States in whose territory the server, the service provider (e.g. e-mail provider), or the nodes of data traffic are located, even in cases where the data merely traverses the territory *en route* to its final destination.[813]

The broadest stretch of the territoriality principle is provided by the so-called "effects doctrine", which allows the allocation of jurisdiction over offences having a substantial effect on the

---

[808] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 233. Cfr UNODC, *Comprehensive Study on Cybercrime* (n 66), 190. See also EU, *2005 Framework Decision on attacks against information systems* (n. 82), Article 10.2: "When establishing its jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that the jurisdiction includes cases where: (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory."

[809] See: 'Maps of Internet Service Provider (ISP)
and Internet Backbone Networks', <http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/isp_maps.html>.

[810] See: L. Picotti, 'I profili penali delle comunicazioni illecite via Internet', (1999) Diritto dell'Informazione e dell'Informatica 288, 1999; G. Ziccardi, 'Cybercrime and Jurisdiction in Italy', in S. W. Brenner & B-J. Koops (Eds), *Cybercrime and Jurisdiction: A Global Survey* (SPRINGER 2006), 227, 236; C. M. Paulucci, *Cooperazione giudiziaria e di polizia in material penale* (UTET 2011), 725.

[811] See US, *West Virginia Penal Code*, Ann. §61-3C-20 (2004) (emphasis added).

[812] See Singapore, *Computer Misuse Act 2007*, Section 11(3)(b): "For the purposes of this section, this Act shall apply if, for the offence in question (…) the computer, program or data was in Singapore at the material time." (S. W. Brenner & B-J. Koops, 'Approaches to Cybercrime Jurisdiction', (2004) 4 Journal of High Technology Law 1, 20; ITU, *Understanding Cybercrime: Phenomena, Challanges and Legal Response*, (n 66), 236).

[813] See M. N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 801), 55. The Group of Expert was, however, highly critical with respect to such mean of application of jurisdiction, highlighting the lack of a substantial effect on the territory of the State.

territory of the State[814]. This controversial criterion[815] is based on a link with the prosecuting State provided only by the effect of the act. Contrarily to the ubiquity doctrine, the effects doctrine does not necessitate that at least a part of the act is committed intra-territorially. Consequently, it offers to the domestic criminal law a vast *extra moenia* reach.

However, in cyberspace, the distinction between various formulations of the principle loses most of its significance.[816] The subjective/objective territoriality principle gains a far-reaching scope, extended over its typical application in the case of ordinary crimes. The intra-territorial element of the principle is offered by the means of transmission of the crime.

In crimes related to the diffusion of illegal content – such as defamatory, racist, homophobic or pornographic content[817] – the result of the crime takes place on the computer screen where the prohibited information is displayed. While defamation creates minor jurisdictional problems – since it is usually directed against one or a few precise persons – hate, political, or opinion crimes committed online may generate more serious issues. *In primis,* since these crimes virtually have a worldwide reach, multiple States may simultaneously exercise their jurisdiction – grounded on the doctrine of ubiquity – over the act. Furthermore, the criminalisation of these acts highly depends on political or cultural considerations (sometimes related to history – e.g. Nazi apology), and on the extent of the protected freedom of speech. A risk thus exists for the individual to be prosecuted for a conduct that does not constitute a punishable offence in the country where he/she is acting. Far from being exclusively theoretical, concrete cases are paradigmatic on this issue.

---

814 The effect doctrine is sometimes considered as part of the objective territoriality principle (see, e.g. CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (n 797), 8, 24; J. Paust *et al* (Eds), *International Criminal Law: Cases and Materials* (Carolina Academic Press 1996), 124-126; CoE, *Discussion Paper (prepared by H. W. K. Kaspersen), Cybercrime and Internet Jurisdiction*, 5 March 2009, at 9), some other as a separate subprinciple of the principle of territoriality (See UN GA, *United Nations Report of the International Law Commission* (n 795), 522), more oriented towards the protective principle (ITU, *Understanding Cybercrime: Phenomena, Challanges and Legal Response* (n 66),237). This doctrine is notably endorsed by the US federal system (see US, *Restatement (third) of Foreign Relations Law,* §402, "… a State has jurisdiction to prescribe law with respect to (…) conduct outside its territory that has or is intended to have substantial effect within its territory".

815 See CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (n 797), 24; M. Hayashi, 'The Information Revolution and the Rules of Jurisdiction in Public International Law', in M. Dunn Caventy et al. (eds), The Resurgence of the State: Trends and Processes in Cyberspace Governance (Routledge 2007), 13, 64.

816 *Id.,* 59, 68 ff..

817 See, *inter alia*, ITA, Corte di Cassazione, *Judgement n. 16307/2011* "…the locus commissi delicti of the telematics defamation is located in the place where the offences and the denigrations are perceived (…) even if the website is registered above, if the offence is perceived by users that are located in Italy".

For instance, in the Toblen case[818], the German Federal Court of Justice held the applicability of § 130 points 1 and 3 of the German Criminal Code (criminalising hate incitement and Nazi apology)[819] to an Australian website containing revisionist opinions. According to the Court, due to the accessibility of the website from Germany, the result of the crime happened in German territory.[820] Besides the evident importance of an extensive criminalisation of anti-democratic ideas, it should be noted that the broad extension and multiplication of jurisdictions in cases of hate, political and opinion crimes may lead to minimising "digital" freedom of speech to the most restrictive system, in which the author of digital expression may be prosecuted[821].

Flag Principle.

According to the flag principle, a State has criminal jurisdiction over offences committed on board aircraft or ships registered in ("flying the flag" of) that State. The majority of States recognise this principle.[822] It is envisaged by the CoE Convention on Cybercrime[823] as a legitimate ground for the exercise of a State's jurisdiction. Conversely, the EU instruments on cyberattacks do not contain the flag principle.

During the drafting of the CoE Convention, consideration was given to including satellites as *loci* covered by the variants of the territorial principle.[824] Since satellites are used as a mere

---

[818] See also the Yahoo! Case, which involves a sale of Nazi-related items on the US Yahoo! Auction website, prohibited in France by Article R645-1 of the Penal Code (see: R. August, 'International Cyber-jurisdiction: A Comparative Analysis', (2002) 39 American Business Law Journal 531, 531-532; M. Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace', (2006) 6 In Law 284, 290-293).

[819] "Incitement to hatred – (1) Whosoever, in a manner capable of disturbing the public peace: 1. incites hatred against segments of the population or calls for violent or arbitrary measures against them; 2. assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population; shall be liable to imprisonment from three months to five years. (…) (3) Whosoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of International Criminal Law, in a manner capable of disturbing the public peace shall be liable to imprisonment not exceeding five years or a fine." (translation by Prof. Dr. M. Bohlander, available at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1200).

[820] See GER, *Bundesgerichtshof, Urt. v. 12. 12. 2000 – 1 StR 184/00, (LG Mannheim), NJW 54(8), 624–628, 2001*. For an analysis of the case see M. Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' (n 818), 293-295.

[821] See C. T. Murphy, International Law and the Internet: An Ill-Suited Match, (2002) 25 Hastings International and Comparative Law Review 405, 415-416. Moreover, it may conflict with the predictability requirement (see *infra* n 845). Yet, does the global dimension of the web encompass predictability of criminalisation? When a person acts on the web (for example creating a website), does he/she have clearly in mind the territorial extension of its act, and the global reach of the Internet?

[822] See US, *Lauritzen v. Larsen*, 345 U.S. 571, 585 (U.S. 1953); The Netherlands: A. Klip (ed), *Substantive Criminal Law of the European Union* (n 144), 106; FR, *Code Pénal*, Art. 113-3, 113-4.

[823] CoE, *Convention on Cybercrime* (n 81), Article 22 (b) (c).

[824] See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 234.

conductor for the flux of data, the drafters considered that, in the majority of cases, they would not serve as an appropriate basis for jurisdiction, lacking the necessary nexus for most States.

However, flag States retain jurisdiction over satellites in outer space.[825] States that exercise their jurisdiction over an act on the basis of the mere transit of a flux of data through its territory[826] may indeed exercise their jurisdiction on the base of the "nationality" of a satellite touched by the *iter criminis*.

Further, a satellite is constituted by its "flying part" and its ground station. Given a sufficient nexus with the State according to its domestic law, jurisdiction may be theoretically based on the location of the ground infrastructure.[827]

The importance of the flag principle as a basis for exercising jurisdiction may prospectively grow. Soon, naval or aerial vehicles controlled by computer systems (e.g. drones) may become a frequent target of cyberattacks[828]. In these cases, the State where the ship or aircraft is registered may indeed base its jurisdiction on the flag principle.

Personality Principle (active and passive).

Personality (or nationality) based principles establish the exercise of jurisdiction on the nexus between the nationality of the offender (active personality) or the victim (passive personality) and the prosecuting State.

---

[825] See UN GA, Resolution 1962 (XVIII), *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, 13 December 1963, § 7 (Such a resolution may be deemed to represent an expression of sufficient *usus* and *opinion iuris seu necessitatis* to constitute customary law, see: B. Cheng, "United Nations Resolutions on Outer Space: 'Instant' International Customary Law?" (1965) 5 Indian Journal of International Law 23). See also UN, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, UN GA Resolution 2222 (XXI), annex, 19 December 1966, Article VIII.

[826] See *supra* principle of territoriality, and n 810.

[827] See S. W. Brenner and B-J. Koops, 'Approaches to Cybercrime Jurisdiction' (n 812), 16. According to these commentators, jurisdiction over satellites may be based on the principle of protection, since the States may "want to protect their technology and property from being abused for criminal reasons" (*idem*, 27). In the view of the author of this work, several continually repeated acts impairing the functioning of the satellite may indeed trigger the principle of protection. A single act using the satellite as a mean of propagation, on the other hand, cannot be considered as damaging an "essential" fundamental interest of the State. Thus, applying jurisdiction on the basis of this principle may constitute a too broad stretching of its scope (See, *ex plurimis*, M. N. Shaw, *International Law* (n 796), 667).

[828] See: P. Paganini, 'Hacking Drones: Overview of the Main Threats' (Infosec, 4 June 2013) <http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats>; Glenn Sanders, 'The Very Real Dangers of Hacked Drones' (Tractica, 4 September 2019) < https://www.tractica.com/robotics/the-very-real-dangers-of-hacked-drones/>. See also: Anonymous operation, 'How to kill drones' <http://anoncentral.tumblr.com/post/42515581659/how-to-kill-drones>.

The well-established principle of active personality[829] is grounded on the power of the State to regulate the conduct of its nationals even when abroad, and it is often conditioned by the double criminality requirement.[830] The principle appears to be extremely useful in avoiding impunity when the domestic law provides for the exclusion of nationals from extradition.[831]

This jurisdictional ground is envisaged by the CoE Convention,[832] and by the EU instruments on cyberattacks. The provision contained in the EU instruments covers the cases of the offence being committed both by a citizen and for the benefit of a legal person that has its head office in the territory of the Member State.[833] Such a variant of the principle is strictly related to the provisions on the liability of legal persons for the commission of offences referred to in the EU instruments, principally aimed at repressing cyber economic espionage.

The passive personality principle finds its rationale in the State's duty to protect its citizens.[834] Although highly disputed in the past,[835] it is now widely recognised,[836] specifically with regard to crimes such as terrorism[837] and crimes against minors.[838] In relation to cybercrimes, in particular in the case of attacks against public interest websites (e.g. a website that has thousands of international users), the scope of application of the principle may be overly dilated. Imagine the theft of user data from a leading video-game company.[839] Such an attack may involve victims from all over the world. Under the passive personality principle, it will theoretically

---

829 See UN GA, *United Nations Report of the International Law Commission* (n 795), 523. For the US system see: US, *United States v. Blackmer*, 284 U.S. 421, 437 (1932). For the German system: GER, *Strafgesetzbuch,* § 7.2.

830 See, e.g.: CoE, *Convention on Cybercrime* (n 81), Art. 22(1)(d) (save the case when the offence is committed outside the territorial jurisdiction of any State).

831 See, e.g., GER, *Grundgesetz für die Bundesrepublik Deutschland*, Article 16; FR, *Law of 10.3.1927 on the French extradition*, Article 3.

832 CoE, *Convention on Cybercrime* (n 81), Art. 22(1)(d).

833 EU, *2005 Framework Decision on attacks against information systems* (n. 82), Article 10.1.b; EU, *2013 Directive on attacks against information systems* (n 83), Article 12.3.b. In the EU Directive, the principle of a benefit to a legal person is not formulated as an obligation. Rather the State has a duty to inform the Commission in case the jurisdiction is established on the basis of such principle.

834 See M. N. Shaw, *International Law* (n 796), 659.

835 See UN GA, *United Nations Report of the International Law Commission* (n 795), 524; CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (n 797), 12.

836 See International Court of Justice, *Democratic Republic of the Congo v. Belgium*, I.C.J. Reports 2002, 77, § 47.

837 See, e.g., US, *United States v. Yunis*, 681 F.Supp. 896, 1091 (D.D.C. 1988).

838 See EU, *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*, OJ L 335, 17.12.2011, Art. 17(2)(a); CoE, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, ETS No.201, 25.10.2007, Art. 25(2).

839 See: S. Richmond and C. Williams, 'Millions of internet users hit by massive Sony PlayStation data theft' (The Telegraph, 26 April 2011), <http://www.telegraph.co.uk/technology/sony/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html>.

create a multiplication of competent jurisdictions. On the other hand, due to the general difficulty in tracing back the attack and identify the offender (often possible only after lengthy investigations), the passive personality principle may be more easily applied than the active personality principle. Yet, both the CoE Convention and the EU instruments do not provide for the passive personality principle.

Protective Principle.

Well established in international law, the protective principle legitimises the exercising of jurisdiction over acts committed abroad which constitute a threat to the vital interests of the State. Although its borders are not fixed,[840] the protective principle is usually linked to highly fundamental interests of the State related to national security, territorial integrity, or political independence.[841] From a diachronic analysis of the scope of the principle, it is possible to highlight its primary link to politically hostile acts, constituting a threat to national security (especially espionage and terrorism).[842]

One of the core elements of the principle may be deemed to be the self-defence of the State and its political order. The scope of the principle may easily cover acts of (physical or digital) political activism, dissidence and protest conducted abroad that may "threaten" the political order of the State.

Among the existing binding instruments on cybercrime, the principle of protection is envisaged only by the League of Arab States Convention. In the case of jurisdictional conflicts, the Convention recognises precedence to States exercising their jurisdiction based on this jurisdictional ground.[843]

---

[840] See, e.g., M. N. Shaw, *International Law* (n 796), 667.

[841] See, e.g., US, United States v. Ben Laden (92 F. Supp. 2d 189 (S.D.N.Y. 2000); FR, Cour de Cassation, *in re Urios* 1919-1922, Ann. Dig. 107, No. 70; UK, *Joyce v. Director of Public Prosecution*, ([1946] AC 347). See also: Note, 'Limitations on the Federal Judicial Power to Compel Acts Violating Foreign Law', (1963) 63 Columbia Law Review 1441, 1474-75 (linking the principle to the "political or financial security of the State"); Harvard Research in International Law, *Draft Convention on Jurisdiction with Respect to Crime*, (1935) 29 American Journal of International Law 435, 543 (linking the principle to the concepts of the security, territorial integrity or political independence of that State); B. Simma and A. T. Muller, 'Exercise and limits of jurisdiction,' in J. Crawford *et al* (eds), *The Cambridge Companion to International Law* (CUP 2012), 143-144 (linking the principle to the government power: "acts that severely jeopardise a state's government function").

[842] See FR, Cour de Cassation, *in re Urios* (n 841), regarding espionage of French information to Spain; UK, *Joyce v. Director of Public Prosecution* (n 841), regarding broadcasting pro-German propaganda in England from a third country during World War II; US, United States v. Bin Laden (n 841), founding the extraterritorial application of the Anti-Terrorism Act on the protective principle.

[843] LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 30.

IV.II.II. CONFLICTS OF JURISDICTION.

The transnational character of cybercrime, coupled with the expanded scope of application of the traditional principles of jurisdiction, may lead to a peculiar accumulation of applicable laws and competing criminal jurisdictions over the same act. Many States can exercise their prosecutorial authority; thus, multiple procedures *in idem*[844] can be initiated.

The perpetrators may not foresee this accumulation of competing jurisdictions. For instance, they may be unaware of the exact location of the devices involved, or the jurisdictions touched by the crime. This accumulation can thus create a *vulnus* to the fair expectation of the individual to know where, and if, he/she might be prosecuted and with which law he/she must comply.[845]

Furthermore, accumulation of competing jurisdictions may lead to a risk of multiple punishments, conflicting with the principle of *ne bis in idem,* according to which nobody can be tried or convicted twice for the same offence. The principle, however, finds application only

---

[844] The issue of whether the prosecutions or trials are based on an *idem* may be considered according to three main approaches: focusing on the identity of the facts, their legal characterisation, or the existence of essential elements common to both offences. See, in particular, on *idem* as *idem factum* – thus disregarding the legal classification of the offence contested – the case-law of the ECtHR on Article 4 Protocol No. 7, in particular *Sergey Zolotukhin v. Russia* (Application n. 14939/03), 10 February 2009, (Grand Chamber), in which the Court held that Article 4 should be understood as prohibiting the prosecution or trial for a second "offence", when it arises from the same facts (or facts that are "substantially" the same) as those underlying the first offence.

[845] The negative theory of legality postulates the protection of the individual against aggressive and unexpected prosecution. He/she must know in advance what conducts are prohibited and will trigger criminal prosecution (see, *inter alia*, G. P. Fletcher, *Basic concepts of Criminal Law* (n 143), 207; A. Ashworth, *Principles of Criminal Law* (n 433), 63-66, 2009; US, *Grayned v. City of Rockford* - 408 U.S. 104, 108 [1972] "Because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly"). Specifically, the predictability requirement works as a restraint to a broad application of the territoriality principle (See: CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (n 797), 22 ff.; CoE, *Discussion Paper (prepared by H. W. K. Kaspersen), Cybercrime and Internet Jurisdiction* (n 814), 9. See also, regarding the predictability requirement concerning hate/opinion crimes *supra* n. 821).

within the same national legal order[846] or, in some cases, at the regional level.[847] Usually, the principle is activated after a State's judicial authority has rendered an enforceable verdict, leaving an active "net" of competing jurisdictions to cover the act. This situation decreases the efficiency of the administration of justice and leads to unnecessary costs for the States and for the offender, who is left in the "uncomfortable" situation of being ignorant of where and if he/she can be prosecuted or sentenced.

Essentially, there are two models for governing the possible jurisdictional conflicts arising when two or more States are willing to exercise their criminal law over the same act. Firstly, envisaging the need for the involved States to cooperate at various stages, with the aim of concentrating the jurisdiction in one particular State.[848] Secondly, providing for a list of criteria of prevalence for determining which is the competent State.

The *ex ante* approach to the issue – based on the identification of the competent jurisdiction by means of a hierarchical list of prevalent criteria – is aimed at providing simplification, certainty over the applicable law, and avoidance of unnecessary vexation to the person in terms of multiple prosecutions or ambiguity as to the law with which they must comply. Conversely, the other model seeks to resolve the issue at a later stage, when the offence is already committed, and the competing jurisdictions triggered, mainly through providing for consultation and cooperation between prosecuting authorities.

The CoE and EU systems have adopted the latter solution, which is focused on efficiency in terms of repression. It avoids impunity through the activation of several parallel jurisdictions, but it subjects the suspect to concrete risks of multiple prosecutions. Although aimed at concentrating jurisdiction in one State, simple mechanisms for communication, not supported

---

[846] Although the principle is recognised in international instruments, these provisions have been interpreted as being limited to the an internal *ne bis in idem* (see, CoE, *European Convention on Human Rights*, *Seventh Additional Protocol*, ETS 117, 22 November 1984, Article 4; Human Rights Committee case law on Article 14, paragraph 7 of the International Covenant on Civil and Political Rights [A.P. v. Italy, 16 July 1986, Communication No.204/1986, CCPR/C/31/D/204/ 1986, para. 73]. See also: Belgium, Hof van Cassatie - Cour de Cassation,*20 February 1991*, 131; ITA, Corte di Cassazione, *Judgement n. 44830/2004*). However, the Dutch Penal Code contains a general *ne bis in idem* provision that is applicable to domestic and foreign judgments, regardless of the place where the offence was committed, thus giving an international scope to the principle (see: P. Baauw, 'Non bis in idem', in B. Swart & A. Klip, International Criminal Law in The Netherlands (Edition Iuscrim 1997), 75.

[847] In the EU, the principle is enshrined in Article 54 of the EU, *Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders*
OJ L 239, 22/09/2000, and Article 50 of the EU, *Charter of Fundamental Rights of the European Union,* OJ C 326, 26.10.2012.

[848] Cfr also the criterion of "reasonableness" of US, American Law Institute, *Restatement (3rd) of Foreign Relations Law,* § 403.

by a central body,[849] may appear to be ineffective in cases where States are unable to reach a consensus on which of them should have prevalence.

With regard to cybercrime, the expanded applicative scope of the traditional jurisdictional principles may generate a concrete risk of a multiplication of enforceable laws. Particular attention in the application of the principles of jurisdiction, coupled with a mechanism of prevalence and strict coordination between investigating authorities, may avoid conflicts of jurisdiction.

However, existing multilateral instruments do not satisfyingly address the problems deriving from the apparent unsuitability of the conventional rules of jurisdiction on cybercrime, nor those related to the possible consequent conflicts of jurisdiction.

EU Framework Decision 2005/222/JHA on attacks against information systems do envisage a system for regulating conflicts of jurisdiction based both on cooperation and on criteria of prevalence. According to Article 10.4 "where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors: the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2, the Member State shall be that of which the perpetrator is a national, the Member State shall be that in which the perpetrator has been found." However, this jurisdictional clause was not transposed in the subsequent Directive 2013/40/EU, repealing Framework Decision 2005/222/JHA, which does not contain any methods for resolving conflicts of jurisdictions.

The CoE Convention envisages a simple consultation mechanism, while a list of criteria to allocate jurisdiction is lacking.[850] Article 22.5 of the CoE Convention states that "the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution". Criteria for the determination of the competent State are instead provided for in the LAS Convention. Precedence is given to: firstly "the State whose security or interests were disrupted by the offence", secondly "the State in whose territory the offence was

---

[849] See, for instance, the role of Eurojust in the conflicts of jurisdiction within the EU (I. Patrone, 'Conflicts of jurisdiction and judicial cooperation instruments: Eurojust's role', (2013) 2 Era Forum 215).

[850] See CoE, *Discussion Paper (prepared by H. W. K. Kaspersen), Cybercrime and Internet Jurisdiction* (n 814), 20.

committed" and finally "the State of which the wanted person is a national".[851] In case of jurisdictional claims based on similar linking factors, the first State that requests extradition shall have priority. Interestingly, the Arab Convention grants priority to the protective principle over the traditionally stronger territoriality principle.

More generally, in the European Union system, the problem of concurrent jurisdictions is addressed by Framework Decision 2009/948/JHA[852] aimed at promoting exchange of information and direct consultation between the authorities involved in order to prevent and settle conflicts of jurisdiction. If the procedure indicated by this instrument does not lead to a consensus between the conflicting proceeding authorities, the Framework Decision provides that the matter shall be referred to Eurojust by any competent authority of the Member States involved.[853] One of Eurojust's main tasks is to foster cooperation between judicial authorities. According to Article 6 of the so-called "Eurojust Decision"[854], the agency has the power to ask a proceeding authority to "accept that one of them may be in a better position to undertake an investigation or to prosecute specific acts".

From a normative point of view, the European system of jurisdictional conflict resolution finds its cornerstone in the *ne bis in idem* provision of the Schengen Convention[855]. The same principle is also enshrined in Article 50 of the Charter of Fundamental Rights of the European Union[856]. Notwithstanding the attention on the prevention of conflicts – see, for instance, 31(1)(d) of the Treaty on European Union (TEU) – the individual is protected from a second prosecution for the same act only after a Member State delivers a final judgment. No binding criteria facilitate the choice of the most appropriate forum. The European system is thus focused on the value of the final judgment – *res judicata pro veritate habetur* – while putting in the background the risk that the individual may be subjected to multiple prosecutions to their detriment – *nemo debet bis vexari pro una et eadem causa.*[857]

---

851 LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 30.3.

852 EU, *Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings*, OJ L 328, 15.

853 …provided that Eurojust is competent to act ratione materiae.

854 EU, *Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*, OJ L 138, 4.6.2009.

855 EU, *Convention implementing the Schengen Agreement* (n 847), Articles 54-58.

856 EU, *Charter of Fundamental Rights of the European Union,* (n 847), Article 50.

857 See C. Van Den Wyngaert and G. Stessens, 'The international non bis in idem principle: resolving some of the unanswered questions', (1999) 4 International and Comparative Law Quarterly 779, 780-781.

However, such an *ex post* system would not easily be applied on a global scale, in particular because a universal *ne bis in idem* principle is lacking. Many States, especially Romano-Germanic systems, refuse to recognise the *res iudicata* value to foreign judgments.[858]

Furthermore, at the global level, problems may arise concerning what constitutes an *idem*.[859] If an identical legal classification of the facts has to be considered as *idem*, in the absence of a sufficient degree of harmonization, legal systems with significant differences in the cybercrime framework may encounter problems in considering whether the two criminal offences coincide, thereby creating the risk of double prosecution. Conversely, *idem* intended as same facts may prevent prosecution even if the first judgment has been held on the basis of lesser charges (or, for instance, of legislation unable to satisfyingly cover cybercrimes).[860] However, it may possibly leave the retributive interest of the second State dissatisfied, and eventually create the risk of substantial impunity.

Given all of the above, a reformulation of the scope of the application of the jurisdictional rules concerning cybercrime may still be necessary. In particular, the territoriality principle – based on the concept of territory and constructed via the traditional means of commission of ordinary crimes – seems to lose its accuracy and certainty of application in the face of cybercrime's spatial diffusion.[861] Setting up a minimum threshold for the necessary connection between criminal conduct and prosecuting State may indeed cut out the excessive expansion of this principle.[862]

The evolution of the interpretation and application of the principles of jurisdiction may not be left to separate unilateral approaches by the States. In the case of cybercrime, State jurisdictions are necessarily interconnected. They must be harmonised in order to efficiently respond to the transnational structure of cyberspace and avoid excessive overlapping.

---

858 *Id.*, 783.

859 See *supra* n 844.

860 See, for instance, *supra*, § I.II.II., The Love Bug case.

861 Indeed, a purely territorial jurisdiction seldom finds application in relation to cybercrime, in favour of "qualified" territoriality (ubiquity or effect doctrines), which contains – at various degrees – an extraterritorial element.

862 For example, on the base of the *de minimis* requirement developed by the US Courts (see US, *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); US, *Milliken v. Meyer*, 311 U.S. 457, 463 (1940). See also: J. Hornle, 'The Jurisdictional Challenge of the Internet', in L. Edwards & C. Waelde (Eds), Law and Internet (Hart 2009) 143-144).

IV.III. CYBERSPACE: AN INTERNATIONAL SPACE?

In order to better assess the jurisdictional issues related to cybercrime, it might be interesting to ponder over the concept of "cyberspace" itself. Upon preliminary consideration, it is essential to anticipate three constituent elements of this concept: it is a virtual spatial dimension; it is physically created by the interconnection of digital devices; it is the space in which most cyber offences are committed.[863]

The term "cyberspace" was created in the 1980s by science-fiction authors. The enormous success of the term seems to be connected to its vagueness. Semiologically, "cyberspace" became a container for all new perceptions related to the "virtual reality" that new technologies were generating.

On the one hand, cyberspace, in its ontological nature, can be represented as a virtual spatial superstructure, grounded on particular concepts of space and time, and modulated on electronic impulses. Cyberspace is a place where people meet, store data, find and share knowledge, information, or conduct activities.[864] It is transcendent, and "virtually" covers the physical space; global, crossing the whole planet – earth, sea and sky; to some extent common, as its users share it with people from all over the world; and almost unaffected by the traditional legal and political concepts of territory and borders,[865] on which criminal law has historically been rooted.

On the other hand, this *alter-space* is concretely generated by a physical human-made layer of devices, which materially constitutes cyberspace, and by their specific technical use, which shapes its architecture. Underneath the metaphysical concept of cyberspace lies a "material base" consisting of infrastructures, such as servers or cables, which physically constitute it.

A second point of mirrored correspondence to the real world is provided by its "portals", which are the internet-connected devices through which an individual has access to cyberspace. As the number of connected devices drastically augments,[866] so does the interconnection between

---

863 See generally *infra* I.I. and n 16.

864 See, *infra*, § II.VII. and n 427.

865 It may be affected, for instance by censorships and access restrictions by authoritarian States.

866 According to an analysis conducted by IoT Analytics, in 2018 17 billions connected devices were in use worldwide: 7 billions were Internet of Things devices (K. Lasse Lueth, 'State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating' (IoT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>.

cyber and real space. Such a widespread diffusion of "bridges" is melting the two spaces into a sort of "hybrid space".[867] While cyberspace itself transcends physical territories and geopolitical borders – and, as such, may be considered international – both its "material base" and its "portals" are physically located within the border of States. Hence, they are subject to States' jurisdiction.

The first possible mode of application of a State's jurisdiction over cyberspace is through its physical manifestations. For instance, intercepting data that flow in the State's territory, or prosecuting cybercrimes committed against computer systems located therein.[868]

The territory of a State is defined by its borders, which delimit an area where a given set of rules applies. Such rules are at the same time expression and protection of a *Volkgeist:* a cultural, moral and ethical system of values.[869] Territoriality is the primary principle of criminal jurisdiction, which marks the spatial scope of application of criminal law inside a State's territory. Traditionally, most of the threats to such a system of values derived from acts committed within the State's territory. Giving the extensive spatial possibilities of new technologies as a means to commit crimes, cyber activities conducted in one State may reverberate globally, possibly harming values and interests of every State connected to cyberspace. An Australian individual creates a negationist website, which is accessible in Germany. A Thai hacker steals a credit card number of an American lady. In the lack of sufficient harmonisation and an efficient interstate-cooperation (see, for instance, the Love Bug case)[870], the State may wish to apply its criminal law to conduct that has a substantial effect on its territory, its interests, and its citizens.

When considering jurisdictional issues in cyberspace, the main problem appears to be how to avoid excessive multiplications of applicable criminal laws and jurisdictional conflicts, while satisfying the legitimate claim of a State to protect its citizens and its interests against cybercrime. All the possible answers are necessarily linked to the peculiar spatial characteristics of cyberspace and the scope of its future development.

---

867 See, *supra* n 21.

868 See *supra* § IV.II.I, n 810.

869 See T. Schultz, 'Carving up the internet: jurisdiction, legal orders, and the private/public international law interface', (2008) 4 European Journal of International Law 799, 806ff.

870 See § I.II.II., The Love Bug case.

IV.III.I. CYBERSPACE AS A GLOBAL COMMON.

The first approach to cyberspace, proposed by some commentators, is to consider it as a purely international space, i.e. a "global common"[871]. The territoriality principle of jurisdiction will thus find no application, since no national jurisdictions will be allocated on cyberspace itself. Possibly, as with outer space or the high seas, criminal jurisdiction will be exclusively grounded in the nationality of the "fixed platforms" present in cyberspace (the "material bases" of cyberspace). This approach, however, may lead jurisdiction being almost entirely concentrated (with the obvious related problems) in the States where most Internet infrastructure is located. Additionally, multiplication of applicable jurisdictions may still derive from the fragmentation of data through different servers (for instance, in cloud computing services)[872].

Following the proposed deregulation and "deterritorialisation" of cyberspace as an independent territory, a "re-regulation" appears necessary. Every global common is regulated by an international treaty, which addresses the issues of sovereignty and jurisdiction.[873] However, contrarily to all other international spaces, cyberspace is a living, dynamic, and mutable space. Furthermore, its existence requires a physical technological structure, which is located in the "real world", and is mostly in the hands of private companies. There is, therefore, a risk that such "*pars construens*" may be more an auto- or hetero-regulation of the technical functionalities and aspects of cyberspace, than a concerted and international regulation. Furthermore, such regulation, already existing at the technical level, may have a concrete effect on the various principles of jurisdiction. Their scope may adapt along with technological evolution and modifications in the Internet "architecture": i.e. the way data is stored, the physical location of

---

[871] See, *inter alia*, D. Jerker & B. Svantesson, 'Borders On, or Borders Around—The Future of the Internet', (2006) 16 Albany Law Journal of Science and Technology 343; D. C. Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces', (1998)
4 Michigan Telecommunications and Technology Law Review 69; D. R. Johnson and D. Post, 'Law and Borders -The Rise of Law in Cyberspace', (1996) 48 Stanford Law Review 1367, 1367. See also US, Department of Defence, *US Strategy for Homeland Defense and Civil Support* (2005): "the global commons consist of international waters and airspace, space, and cyberspace".

[872] See *supra* n 40.

[873] See P. W. Franzese, 'Sovereignty in Cyberspace: Can it exist?', (2009) 64 Air Force Law Review 1, 14.

the servers/providers, the technology related to Internet identification and, more generally, the role of "Internet governance"[874] and its future directions.

In any cases, international spaces are traditionally spatially detached from the State's territory, which is hardly touched by the acts committed therein.[875] Very few crimes are committed in the traditional common spaces, apart from crimes of piracy on the high seas – to which, in fact, universal jurisdiction is applied. The State has far more interest in regulating the conduct brought about in cyberspace than in the traditional global common spaces, since cybercrime generates qualitatively and quantitatively serious threats to the State.[876] Furthermore, cyberspace is extensively intertwined with the "real space" through its physical manifestations located within the State's jurisdiction.

The likelihood is that cyberspace will never be considered a completely independent international space. Via the interfaces and the physical devices that form its base, cyberspace is strongly related to the territory of the State, on which cyber conduct will always have a substantial real effect.

IV.III.II. THE BALKANISATION OF THE WEB.

A different solution to the particular spatial characteristics of cybercrime, and to the related jurisdictional problems, is its fragmentation and division into different areas: the so-called "balkanisation" of the Internet.

As a product of human-made technology, the web is prone to being regulated autonomously by States. Intervening in the physical layer of devices that constitute cyberspace, States may erect virtual fences and delimitate areas of the web. Separate areas may be created through the

---

[874] The Working Group on Internet Governance was set up by the Secretary-General of the United Nations, with the aim – *inter alia* – to develop an "adequate, generalizable, descriptive, concise and process-oriented" definition of Internet Governance. In 2005, it provided the following definition: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (UN, Working Group on Internet Governance, *Report of the Working Group on Internet Governance*, 4, 2005 <http://www.wgig.org/docs/WGIGREPORT.pdf>).

[875] See D. Jerker and B. Svantesson, 'Borders On, or Borders Around' (n 871), 366.

[876] See: P. Hyman, 'Cybercrime: It's Serious, But Exactly How Serious?' (Communications of the ACM, March 2013) <http://cacm.acm.org/magazines/2013/3/161196-cybercrime-its-serious-but-exactly-how-serious/fulltext>: "Symantec Corp. reports cybercrime is costing the world $110 billion every year. But, according to McAfee Inc.—Symantec's closest competitor—the actual annual cost worldwide is almost 10 times that, approximately $1 trillion".

placement of a series of filters and firewalls, or the channelling of incoming and outgoing Internet traffic.[877]

A territorial delimitation of cyberspace could likely permit easier identification and geolocalisation of data origin, destination, and movement, and allow control of incoming data, thereby stopping undesired traffic from entering the territory. Furthermore, such delimitation may likely produce tight censorship, which blocks incoming and outgoing data perceived as threats to the national legal, political, moral, and cultural stability. Eventually, it may annihilate freedom of expression and likely induce the political drift of the State. The result would be that the Internet will cease to exist as a free global space of culture and knowledge sharing. This alone represents a serious set of challenges, without even considering the related economic consequences.

Nevertheless, as a resurgence of the Westphalian concept of territory, balkanisation will efficiently protect the State's values. It will block external content that may be considered harmful to a determinate legal and political order. New virtual borders will be created to defend an accepted system of social behaviour against external disturbances. The Internet will likely tend towards a division into national or regional blocks that share common values.[878] This appears to be in line with the new political agenda of many countries.

On the other hand, balkanisation will limit the use of the Internet for political espionage, and surveillance conducted by foreign authorities on citizens' sensible and private data. The impact of the so-called "datagate", NSA surveillance, Russia's digital influence operations and, more in general, the growth in concern about privacy online, may boost this process[879].

Essentially, balkanisation will augment the territorialisation of cyberspace, by rationalising the relation between the physical and virtual space through an increased control on infrastructures, and therefore on location, origin, and destination of data. The creation of multiple controlled

---

[877] See, e.g., the Chinese Golden Shield Project (E. Chan, 'The Great Firewall of China' (Bloomberg, 6 November 2018) <https://www.bloomberg.com/quicktake/great-firewall-of-china>. See also T. Hatmaker, 'Russia plans to test a kill switch that disconnects the country from the Internet' (Techcrunch, 12 February 2019) <https://techcrunch.com/2019/02/11/russia-internet-turn-off-digital-economy-national-program/?utm_source=tcfbpage&sr_share=facebook&fbclid=IwAR0m6sbxmOyH7MJis0PF81vi4YBTgA0L-bad5xq42NOh6ZolOviniVixOkQ>.

[878] Nations of the Shanghai Cooperation Organization signed an agreement in 2008 on cybersecurity cooperation, in which dissemination of "information harmful to social and political, social and economic systems, as well as spiritual, moral, and cultural spheres..." is considered one of the main threats in the field. (See Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*, 2 December 2008 <http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf>).

[879] See I. Brown, 'Will NSA revelations lead to the Balkanisation of the Internet?' (The Guardian, 1 November 2013) <http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet>.

"internets" may diminish the multiplication of applicable jurisdictions, creating virtual, yet real, frontiers.

The "territorialisation" of the Internet may serve as a stable basis for the application of the traditional principles of jurisdiction. It will erect fences and borders to protect the interests of States from undesirable data. Furthermore, it will work as a "fair notice" for the individual, signalling the entrance into a particular jurisdiction and the subjection to foreign laws.

IV.III.III. INDEPENDENT COMMUNITIES IN CYBERSPACE.

Cyber criminal law is necessarily focused on the "fallout" of cyber conduct on particular legal systems, and on the legal interests protected therein. Detaching cyberspace from the State's jurisdiction will lead to the inability of the State to regulate conduct affecting its system. Possibly, cyberspace will not become an independent legal space. However, the idea of an independent, purely international jurisdiction for cyberspace, strongly linked with the utopian libertarian idea of the web[880], is far more intriguing than its balkanisation.

A possible "internationalisation" of cyberspace – at least a partial one – may be related to the emergence of interests entirely residing in cyberspace and acts entirely committed therein. Theoretically, such acts will be free from States' claim to regulate them.

For this purpose, it is interesting to consider the communities internal to cyberspace in which "virtual" crimes are committed (such as the virtual-drug selling described by Neal Stephenson in his novel "Snow Crash")[881] and where cyberspace itself is the *locus commissi delicti*.

Multi-user online environments – "virtual worlds", such as Second Life or Sansar[882] – are spaces that host communities. These virtual spaces have autonomous rules (*rectius:* terms of service), currency, market economy, land ownership, and intellectual property rules.[883] Even (real) States have opened embassies in virtual worlds[884].

---

880 See *infra* n 892.

881 See, e.g.: J. Wolfendale, 'My avatar, my self: Virtual harm and attachment', (2007) 9 Ethics and Information Technology 111; F. G. Lastowka and D. Hunter, 'Virtual crimes', (2004) 49 New York law School Law Review 293. Think, for example, of the sale and consumption of virtual pseudo-narcotics in the "metaverse", described in Stephenson's novel "Snow Crash" (N. Stephenson, *Snow Crash* (Bantam books 1992)).

882 See <www.secondlife.com>; <www.sansar.com>.

883 For property rights in the virtual worlds see US, *Bragg v. Linden Research*, Inc., 487 F.Supp.2d 593 (E.D.Pa., 2007).

884 See S. Bengtsson, 'Virtual Nation Branding: the Swedish Embassy in Second Life', (2011) 4 Journal of Virtual Worlds Research 1.

The first documented virtual crime committed in such communities took place in 1993. In one of the first multiplayer real-time virtual worlds, "LambdaMOO", a user called "Mr. Bungle" performed, through its avatar, an act of "virtual rape" on other users, violating the virtual community rules and allegedly producing actual emotional traumas in the victims.[885] Mr. Bungle's account was terminated, but his/her actions brought no real-life penal consequences.[886]

Today, a large number of virtual crimes can be committed in virtual reality. In virtual life simulation platforms or multiplayer online games, virtual crimes range from property, hate and violent crimes[887], to running illegal activities such as prostitution or gambling[888].

However, such virtual crimes are not entirely exhausted in cyberspace. When a virtual thief, through his/her avatar, steals a valuable object from another user to gain private profit (e.g. stealing a sword in a medieval-style online game), he/she essentially commits the same crime as stealing money from an online bank account. The victims are not "citizens of the web": they direct their expectations of the protection of their emotional wellbeing and their personal property – which they gained through real time spent at their desk and for which they paid real money – to their real community, not to the online community. Correspondingly, perpetrators remain bound to their real community by a social contract that prohibits crimes and provides criminal punishment for any substantial antisocial behaviour.

By surfing the Internet, a person may enter in a virtual system of rules, which regulates their virtual conduct. However, they do not "leave" the territory of the State, entering another exclusive order of values and protected interests. Nor do they currently escape the application of the State's criminal law, while performing acts that are punishable according to that legal system.

Such communities are considered nothing but evolved digital games. The community and the order of values to which the "netizens" [889] belongs are still in the real world. The protection of

---

885 See: J. Dibbell, 'A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society', (1994) Annual Survey of American law 471.

886 *Ibid.*

887 For instance, the Dutch Supreme Court stated that virtual items in online virtual worlds can be classified as "goods" in the meaning of Art. 310 Dutch Criminal Code (theft). See The Netherlands, Hoge Raad der Nederlanden, *HR 31 January 2012, ECLI:NL:HR:2012:BQ9251*. See also *supra* n 295.

888 See, the cyber-brothel created in "The Sims Online": J. Shaefter, 'Sex and the simulated city: virtual world raises issues in the real one' (Michigan News, 27 January 2004) <http://web.archive.org/web/20050716075604/http://www.freep.com/news/mich/sims27_20040127.htm>.

889 The term netizen is a portmanteau of the words citizen and Internet. It generally indicates a user of the Internet. More specifically, it may mean a person that uses the Internet as a medium of political participation and actively works to foster open access to the web and right to freedom of expression within it.

interests harmed by crimes in that space and punishment for antisocial behaviour therein is left to the State. Surely, internal terms-of-service do regulate the conduct brought about in the virtual world. At most, the two systems of rules can be considered as hierarchically ordered. Rudimental internal systems for punishing virtual crimes may be emerging[890], limited to virtual punishment. Such communities do not have any means of using real coercive force against an individual.

One possibility is that the State may neglect to apply its jurisdiction to minor virtual crimes, leaving the resolution of the controversy to the rules indicated by the online community's terms of service. Can a virtual theft, committed in an online community where such conducts are permitted, be brought before a real judge? This is unlikely, because in this case the rules of the online community will influence the characterisation of the conduct in a hypothetical real trial, excluding its blameworthiness. Can the same theft be brought in front of a real judge, if the rules of the online community do not permit such behaviour, but do provide for an internal judicial system, expressly excluding the State's jurisdiction? In such a case, the answer is certainly yes. Notably, such rules cannot legitimise conducts harming a State's legal interests (for instance, child pornography). The legal system of the State remains an insurmountable, hierarchically superior, limit.

The rules of any virtual community are not intended to be a completely independent system of law applicable through a "virtual" territorial principle, and excluding other "external" jurisdiction. At least presently, it is not possible to identify any independent interest exclusively protected by a virtual system of criminal law. Even in the case of activities conducted entirely within "virtual reality", the State's jurisdiction finds complete application (according to the traditional principles of jurisdiction).

IV.III.IV. INDUCED UNIVERSALISATION: AN INTERNATIONAL RIGHT TO FREEDOM OF EXPRESSION.

A possible *tertium genus* between balkanisation and internationalisation is possible. This work has extensively considered the process of the universalisation of digital rights and legal goods. The

---

890 See, for instance, the resolution of the "rape in the cyberspace" case (P. Ludlow, 'New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures', in P. Ludlow (Ed), Crypto Anarchy, Cyberstates, and Pirate Utopias (MIT Press 2001), 10ff. See also: J. L. Mnookin, 'Virtual(ly) Law: The Emergence of Law in LambdaMOO', (1996) 2 Journal of Computer Mediated Communication 1.

more rights and values, once "digitalised", acquire an international dimension, the less cyberspace will be subject to State jurisdiction.

The ideal prototype for such proposal/analysis appears to be the right to freedom of expression. This right maintains a focal position with regard to cyberspace. Indeed, it permeates the very utopian idea of the Internet as a free common space shared by all netizens. The famous "Declaration of the Independence of Cyberspace", written in 1996 by John Perry Barlow, founder of the Electronic Frontier Foundation[891], was a response to the enactment of the 1995 US Communication Decency Act regulating pornographic material on the Internet. It proclaims: *"*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather…*".*[892] As a matter of fact, the Communication Decency Act was partially struck down by the US Supreme Court for infringing upon First Amendment free speech rights.[893]

The capacity of digital technology as a means of communication provided worldwide diffusion to digital content, and new particular contours to content-related crimes. The widespread dissemination of content through the web conflicts with the territorial expressions of the freedom of speech, which largely depend on cultural, moral, and traditional values. In fact, almost all of the State's web filters are aimed at blocking particular content (chiefly political and sexual), functioning as a virtual border defending the values of the territory from external "contamination".[894]

To oppose the erection of such fences – but in the apparent impossibility to find a global right to freedom of speech with stable boundaries, outside the broad formulation of Article 19 of the International Covenant on Civil and Political Rights and Article 19 of the Universal Declaration of Human Rights – it is the responsibility of the international community to identify the positive and negative boundaries of a fundamental right to freedom of digital expression. In the context of a legislative reorganisation of cyberlaw issues, cyberspace could be regulated more as an international common space of free, shared culture and knowledge. To

---

891 See Electronic Frontier Foundation <https://www.eff.org>.

892 See J. P. Barlow, 'A Declaration of the Independence of Cyberspace', in P. Ludlow (Ed), Crypto Anarchy, Cyberstates, and Pirate Utopias (MIT Press 2001), 27.

893 See US, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

894 For instance, the UK filters on pornography: K. Bode, 'UK May Have Finally Ditched Its Absurd Porn Filter Plan' (Techdirt, 21 June 2019) <https://www.techdirt.com/articles/20190620/08544442436/uk-may-have-finally-ditched-absurd-porn-filter-plan.shtml>; 'Q&A: UK filters on legal pornography' (BBC, 22 July 2012) <http://www.bbc.co.uk/news/technology-23403068>.

some extent, such a universalisation of the freedom of speech may concretely realise the idea of the Internet as a global common space.

Soft law initiatives on this line already exist. For instance, in 2003, the World Summit on the Information Society adopted, under the auspice of the United Nations, a Declaration of Principles, making specific reference to the importance of the right to freedom of expression in the Information Society. It affirmed that such a right is an essential foundation of the Information Society, and "that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organisation. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits of the Information Society offers."[895]

In 2011, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recognised that "the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression".[896] It also recognised that "legitimate types of information which may be restricted include child pornography (to protect the rights of children), hate speech (to protect the rights of affected communities), defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others), and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life)"[897].

The basic standards for a right of digital expression must, first and foremost, be found in the universal criminalisation of specific conduct. The "negative" core of the international right to cyber-expression is composed of criminal repression instruments.[898] A series of internationally recognised offences delineate its external perimeter. More problems arise in finding a common positive standard for freedom of speech. Even in its international manifestation, freedom of

---

[895] See M. Klang; A. Murray, *Human Rights in the Digital Age*, (Routledge 2005).

[896] UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (n 759), § 20.

[897] *Id.,* § 25.

[898] See, *inter alia*, UN, *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*, UN GA Resolution A/RES/54/263, 25 May 2000; UN, *International Convention on the Elimination of All Forms of Racial Discrimination*, UN GA Resolution 2106 (XX), 21 December 1965, 195.

expression can usually be restricted where necessary for the protection of national security, public order, or morals.[899] The world's political, cultural, and moral values significantly differ. Currently, a "positive" core of universally protected speech will be hard to identify outside regional blocks, which share a common ground. In the future, this idea will profoundly benefit from the process of cultural globalisation led by new technologies. Consequent decreases in historically based differences[900] may create the basic humus for an international digital right to freedom of expression. The Internet self-creates its legal dimension by diffusing cultures.

---

[899] See, e.g., UN, *International covenant on civil and political rights*, UN GA Resolution 2200A (XXI), 16 December 1966, Article 19.

[900] See U U. Sieber, 'The Forces Behind the Harmonization of Criminal Law' (n 138), 400.

IV.IV. TRADITIONAL AND INNOVATIVE TOOLS OF INTERSTATE COOPERATION IN THE FIGHT AGAINST CYBERCRIME.

Cybercrime – and specifically offences committed via the Internet or other types of inter-computer connections – has a typical transnational nature, which is strictly related to the technology employed in the commission of crimes. The offence is usually committed through a connection between devices, and such a connection uses a virtual spatial superstructure, which evades the political or geographic subdivisions of the world.

Cybercrime's preparation, commission, and effect defy national borders[901]. Hence, its prevention, investigation, and prosecution cannot be separated from interstate cooperation.

A "cybercriminal" has virtually (in both its meanings) 4 billion potential victims[902] at a "click's distance". This often means that the offender and the victim(s) are located in different countries[903]; the *corpus delicti* is "stored" in foreign territory; and the crime's traces are scattered across different jurisdictions. When a criminal proceeding is instituted in a State with jurisdiction over a crime, its investigating authorities may need the cooperation of the foreign countries involved.

Cybercrimes are often committed within a very narrow time frame. Wherever located, malicious codes may affect the targeted computer system only "milliseconds after" the beginning of the attack.[904] Digital evidence is extremely volatile and can be deleted or altered quickly and easily. Efficient investigations and prosecutions therefore require an immediate reaction, not only internally, but also in terms of international cooperation.

---

[901] According to the Organized Crime Convention (UN, *Convention against Transnational Organized Crime and the Protocols Thereto (*n 442)), Art. 3(2), "an offence is trans-national in nature if: (a) It is committed in more than one State; (b) It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; (c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or (d) It is committed in one State but has substantial effects in another State".

[902] ITU estimated the number of individuals using the Internet in 2013 (2.7 billion). At the end of 2018, the number rose to 3.9 billion (see ITU, 'Statistics' <https://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx>).

[903] See: UNODC, *Comprehensive Study on Cybercrime* (n 66), 183: "During information gathering for the Study, more than half of countries reported that between 50 and 100 per cent of cybercrime acts encountered by the police involved a 'transnational element.'" (Study cybercrime questionnaire - Q83)

[904] See U. Sieber, 'The Forces Behind the Harmonization of Criminal Law' (n 137), 394.

National investigations and prosecutions in cybercrime cases are highly dependent on the interstate exchanging and gathering of evidence (mutual assistance in criminal matters) and eventually on the transfer of suspects or accused persons for the purpose of criminal investigations or enforcing a penalty or measure (extradition).[905] While efficient interstate cooperation is fundamental to combatting all transnational crime, in relation to cybercrime it assumes particular features aimed at satisfying the needs of cybercrime.

In the investigation and prosecution of criminal cyber activities of a transnational nature, investigating authorities may request the assistance of the State having enforcement jurisdictional competence pursuant to an existing legal or political basis regulating mutual cooperation between them.

Aside from exceptional instances where the State may lawfully exercise its extraterritorial enforcement jurisdiction (which will be considered *infra*), investigative or coercive measures aimed at the investigation and prosecution of cybercrimes involving persons, objects and cyber activities located outside the State territory do require the assistance of the foreign State having enforcement jurisdictional competence. Cooperation in the investigation and prosecution of cyber activities may also involve International Criminal Tribunals, when the act possesses the necessary constituent elements (also in terms of scale and effect of the attack)[906] of an offence falling under their jurisdiction.[907]

The international cooperation framework encompasses two correlated aspects. On the one hand, an internal procedural aspect relates to the procedure to be followed by the requesting and requested parties and is therefore mainly regulated by their national law. The external aspect, on the other hand, mainly relates to mutual relations between sovereign entities. Cooperation between States has a consensual basis, expressed through international treaty law or diplomacy, and is grounded on the principle of sovereignty and its corollaries.

Assistance to a requesting State may be granted pursuant to a treaty or another form of legal or political international agreement (such as a bilateral memorandum of agreement) or on an *ad hoc* basis. States may be parties to several frameworks for international cooperation, the

---

[905] Other tools of interstate cooperation are the transfer of proceedings and the transfer of enforcement of criminal judgments, which, however, remain outside the scope of this work.

[906] See *supra* II.VI.

[907] Cooperation with International Criminal Tribunals is grounded either on a treaty (see UN, Rome Statute of the International Criminal Court, UN A/CONF.183/9 (1998)) or on a binding UN Security Council resolution (see ad hoc International Criminal Tribunals established under Chapter VII of the Charter of the United Nations). See, *inter alia*, A. Cassese and P. Gaeta, *Cassese's International Criminal Law* (OUP 2013), 298ff.

hierarchy of which may be regulated by the traditional principles of *lex superior*, *lex posterior* and *lex specialis*, save express provisions of a different criterion in the applicable instruments.[908]

While there is no universally applicable treaty regulating interstate cooperation, a criminal cyber activity in relation to which cooperation is sought may fall within the substantive scope of a range of applicable instruments. There may, for instance, be broad general agreements on cooperation in criminal matters, or specific agreements limited to particular offences.

Various international and regional cybercrime suppression treaties contain international cooperation provisions expressly designed to address cyber criminal activities.[909] Among the European instruments on cybercrime, only the CoE Convention contains specific provisions on international cooperation mechanisms. Both EU instruments on attacks against information systems, conversely, merely contain a provision on informal cooperation between investigating authorities. However, in the absence of bases and applicable forms of international cooperation in criminal matters, States may resort to noncriminal instruments, such as administrative orders.[910]

In customary international law, there is no general obligation to render assistance in the investigation and prosecution of a crime, including cybercrime. Rather, States engage in specific forms of assistance where provided by a basis regulating cooperation between them, which sets out their scope, limits, and grounds of refusal.

---

[908] See R. Zimmermann, *La coopération judiciaire internationale en matière pénale* (Stämpfli 2009), 185ff. See also, e.g., CoE, *European Convention on Extradition*, ETS 24, 13 December 1957, Article 28; CoE, *Convention on Cybercrime* (n 81), Articles 23 and 27; CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 262.

[909] These conventions either regulate international cooperation extensively, providing for specific cooperation mechanisms (see, e.g., CoE, *Convention on Cybercrime* (n 81); LAS, *Arab Convention on Combating Information Technology Offences* (n 240)), or exclusively impose a general obligation to cooperate expressed in broad terms (see e.g. Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security* (n 878), Articles 3-5. African Union, *Convention on Cyber Security and Personal Data Protection* (2014), Article 28, set out an indirect duty, providing that States "shall undertake to encourage the signing of agreements on mutual legal assistance" and "shall make use of existing means for international cooperation").

[910] However, these bases usually do not envisage the traditional limits to cooperation. This lack may lead to excessive compression of the rights of the sought person/suspect/accused. Circumvention of traditional modes of cooperation is however rarely contested in trial (see, for instance, on the male captus bene detentus principle, C. Paulussen, *Male captus bene detentus? Surrendering Suspects to the International Criminal Court* (Intersentia, 2010)), although in some legal systems it may lead to the exclusion of evidence from trial. See generally M. Cherif Bassiouni, *International Criminal Law: Multilateral and Bilateral Enforcement Mechanisms, Volume 2* (BRILL 2008), at 23.

IV.IV.I. TRADITIONAL FORMS OF COOPERATION.

Extradition.

Extradition is a traditional cooperation mechanism aimed at the surrender of a person accused or convicted of a crime, in order to stand trial or serve a sentence.[911] Besides limits and grounds for refusal provided for by the basis of cooperation, extradition may be limited to enumerated crimes or offences exceeding a certain threshold of gravity.

Specifically, extradition for cyber offences can be regulated by bilateral or multilateral agreements in force between the States involved. The Council of Europe Cybercrime Convention (and the League of Arab States Convention)[912] contains specific provisions on extradition. When both States involved in an extradition process are parties to the convention, and the crime falls under its substantive scope, these provisions find application. The CoE Convention oblige the States parties to consider the offences contained therein as extraditable.

Extradition may be subject both to the substantive scope of the agreement and to a gravity threshold. In particular, in the CoE Convention on Cybercrime the threshold is set to a deprivation of liberty for a maximum period of at least one year or by a more severe penalty, unless a different minimum penalty is provided by an alternative extradition basis applicable between the parties[913].

However, the CoE Convention does not envisage any specific regime of extradition. It merely states that extradition shall be subject to the conditions provided for by the law of the requested Party, or by any applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.[914]

The main aim of such provisions is to offer a legal basis for extradition where no extradition treaty is applicable between the parties[915], and to require the member states to consider the offences contained therein as extraditable under any extradition treaty (existing or future) between them.[916]

---

911 Generally, on extradition, see M. Cherif Bassiouni, *International Extradition: United States Law and Practice* (OUP 2014).

912 Which substantially follows the structure and content of the CoE Convention on Cybercrime.

913 CoE, *Convention on Cybercrime* (n 81), Article 24.

914 *Idem,* Art. 24.5.

915 *Idem*, Art. 24.3.

916 Cfr LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Art. 31.2.

Mutual Assistance.

Cybercrime investigations often transcend national borders. Electronic evidence may be (and usually is) stored on computers, electronic devices, or servers[917] located in one or multiple foreign jurisdictions. Therefore, investigative authorities may need to obtain the cooperation of a foreign country aimed at the implementation of procedural activities (such as enforcement of criminal orders and, in particular, gathering evidence) outside its enforcement jurisdiction (mutual assistance *stricto sensu*).[918]

Moreover, due to the extreme volatility of electronic evidence – which can be deleted, modified or relocated in seconds – the investigative response have to move with a speed that cannot be guaranteed by traditional forms of international cooperation.

The scope of mutual assistance is related to the substantive extension of the applicable legal framework and, given a sufficient degree of flexibility, to the procedural assistance activities explicitly or implicitly envisaged by it.[919]

A number of cybercrime treaties provide for recourse to traditional mechanisms of mutual assistance.[920] Three multilateral agreements on cybercrime (the Commonwealth of Independent States Agreement, the Council of Europe Cybercrime Convention, and the League of Arab States Convention) contain a general provision on mutual assistance, which is to be applied for the purposes of investigations or proceedings concerning criminal offences within the scope of the relevant treaty. The CoE Convention extend its scope of application to the general "collection of evidence in electronic form of a criminal offence"[921]. Additionally, it expressly provide for a series of grounds for refusal: grounds provided for by the law of the requested

---

917 Or even, increasingly, in "clouds" (See, inter alia: CoE, Discussion Paper (Prepared by Research Centre on IT and Law), *Cloud computing and its implications on data protection*, 2010; G. Vaciago, 'Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics', in *CYBERLAWS 2012, The Third International Conference on Technical and Legal Aspects of the e-Society* (Berntzen 2012).

918 See, generally, M. Cherif Bassiouni (Ed), *International Criminal Law: Multilateral and Bilateral Enforcement Mechanism* (Martinus Nijhoff Publishers 2008), Chapter 4: Judicial Assistance and Mutual Cooperation in Penal Matters.

919 See, e.g., the unsuccessful Estonian cooperation request to Russia in the aftermath of the 2007 cyberattacks, in E. Tikk and K. Kaska, 'Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons', in J. Demergis (Ed), *ECIW2010 - 9th European Conference on Information Warfare and Security* (Academic Publishing Limited 2010), 288-294.

920 Commonwhealth of Indipendent States, *Agreement on Cooperation on Combating Offences related to Computer Information* (2001), Articles 5 and 6; CoE, *Convention on Cybercrime* (n 81), Articles 25 and 27; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Articles 32 and 34. The CoE and LAS conventions envisage that the requested Party may make the supply of information or material in response to a request dependent on conditions of confidentiality and limitation on use (CoE, *Convention on Cybercrime* (n 81), Article 28; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 34.7).

921 CoE, *Convention on Cybercrime* (n 81), Art. 25.1.

Party or by applicable mutual assistance treaties;[922] lack of criminalisation of the offence for which assistance is sought in both States involved (double criminality);[923] assistance sought for political offences or offences connected with a political offence;[924] requests whose execution may jeopardise the requested State's sovereignty, security, *ordre public* or other essential interests[925].

The CoE Convention envisages requests for mutual assistance conducted via expedited means of communication – including fax or email – provided an essential level of security, with formal confirmation to follow.[926] Further, it provides for the possibility to forward information obtained within the framework of an investigation to another Party when the State considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with the convention, or might lead to a request for co-operation[927]. The State may request the receiving Party to keep the information confidential or to use it under specific conditions.

Furthermore, the CoE Convention envisages the use of specific provisional and investigative assistance tools aimed at addressing temporal and technical needs of cyber investigation and prosecution.

In particular, the convention provides for the following specific modes of assistance with a general scope (not limited to offences established therein): expedited preservation of stored computer data located in the requested State, before submitting a request for mutual assistance;[928] expedited disclosure of preserved traffic data to the requesting State, in order to help that State identify the service provider and the path through which a determinate communication was transmitted;[929] mutual assistance regarding accessing, seizing, securing or disclosing computer data stored within the territory of the requested State (on an expedited basis where there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or where the treaty applicable between the parties and domestic laws provides for

---

[922] *Idem*, Art. 25.4.

[923] *Idem*, Art. 25.5.

[924] *Idem*, Art. 27.4.a.

[925] *Idem*, Art. 27.4.b.

[926] *Idem*, Art. 25.3.

[927] *Idem*, Art. 26.

[928] *Idem*, Art. 29. Interestingly, the dual criminality principle is excluded as a ground to refuse expedited preservation, unless the receiving Party has reasonable grounds to believe that, at the time of disclosure, dual criminality will not be satisfied.

[929] *Idem*, Art. 30.

expedited cooperation);[930] mutual assistance in real-time collection of traffic data;[931] and mutual assistance regarding the interception of content data[932].

These mechanisms are the international cooperation equivalent of the power established for domestic use in the procedural part of the treaty, whose precise analysis can be found in the previous chapter. They are formulated in order to provide each party with the ability to operate specific investigative actions – similar to those envisaged by the CoE Convention for domestic investigations – for the benefit of another party.

Conversely, no EU cyber-specific instruments contain specific provisions on mutual assistance. In the EU, the matter of cooperation in relation to cybercrime cases or, more generally, to digital evidence, is now regulated by the Directive on the European Investigation Order.[933] This Directive is the expression of a new EU comprehensive system for obtaining evidence in cases with a transnational dimension. The system is based on a single cooperation tool known as the European Investigation Order (EIO). EIOs are issued for the purpose of having specific investigative measures carried out in the executing State, in order to gather evidence. With the exception of joint investigative teams and cross-border surveillance, the order has a general scope that applies to all investigative measures aimed at gathering evidence. Such orders therefore also apply to cyber specific measures.

According to the EIO Directive, the issuing state decides the type of investigative measure to be applied by the receiving State. The issuing State also indicates the formalities and procedures to be conducted during the application of the measure, provided that they are not contrary to the fundamental principles of the law of the executing State.[934] According to Article 10, paragraph one of the Directive, recourse to an investigative measure other than that provided for in the EIO is possible where "(a) the investigative measure indicated in the EIO does not exist under the law of the executing State; or (b) the investigative measure indicated in the EIO would not be available in a similar domestic case". The possibility to request specific measures is thus contingent upon the existence of the investigative power in the domestic system of the executing State.

---

930 *Idem*, Art. 31.

931 *Idem*, Art. 33. "Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case".

932 *Idem*, Art. 34. "To the extent permitted under their applicable treaties and domestic laws".

933 EU, *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters* (n 611).

934 *Id.,* Article 9.

However, paragraph two provides for an exception to this ground for recourse to different types of investigative measures, with specific regard to "(…) (d) any non-coercive investigative measure as defined under the law of the executing State; (e) the identification of persons holding a subscription of a specified phone number or IP address", which "always have to be available under the law of the executing State". On paper, it thus appears that requests for most cyber-specific investigative tools should always be executed by the receiving State, following the type of measure, the formalities, and the procedures indicated by the issuing State.

IV.IV.II. INFORMAL TOOLS OF COOPERATION.

Informal cooperation is a necessary tool to stimulate a fast reaction to cybercrime. A quick response, impossible to achieve through traditional forms of interstate cooperation – which naturally requires time to be processed – is necessary to avoid problems in the investigation generated, for instance, by the loss of digital evidence, which can be easily erased, modified or relocated.

Primarily, informal cooperation is achieved through the use of always-available points of contact, aimed at guaranteeing a fast connection (usually via email or telephone) between investigative authorities. Such points of contact are typically called 24/7 networks.[935]

The first 24/7 network aimed at fast informal cooperation in cybercrime matters was created by the G8 Subgroup on High-Tech Crime. Similar networks are established, *inter alia*, by Interpol[936], by Europol[937], by the Council of Europe Cybercrime Convention[938], and by the League of Arab States Convention on Combating Information Technology Offences.[939] Although not establishing a specific point of contact, the EU instruments on cybercrime exhort the parties to make use of the existing networks.[940]

---

935 See, in general, CoE, Discussion paper (prepared by P. Verdelho), *The effectiveness of international co-operation against cybercrime: examples of good practice* (2008).

936 See Interpol, 'Fact Sheet, Connecting police: I-24/7', COM/FS/2011-02/GI-03 (2001).

937 See: Europol, '24/7 Operational Centre' <https://www.europol.europa.eu/content/page/operational-centre-1853>.

938 CoE, *Convention on Cybercrime* (n 81), Art. 35.

939 LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Art. 43.

940 EU, *2013 Directive on attacks against information systems* (n 83), Article 13; EU, *2005 Framework Decision on attacks against information systems* (n. 82), Article 11.

The main objectives of these operational networks are to offer technical or legal assistance to the competent authorities of the relevant States[941] and to provide direct and near-immediate communication between them, with the aim of facilitating or even directly carrying out[942] the preservation of data, collection of evidence, and location of suspects.[943]

24/7 networks may function primarily as a starting point from which to promote and trigger subsequent formal cooperation (in particular, expedited tools of mutual assistance).[944] Further, due to the broad reach of the existing networks[945], 24/7 networks may serve as a connection between States that do not share applicable legal mechanisms of judicial or investigative cooperation.[946] Being "informal", this mode of cooperation is often subject to "unwritten rules"[947]. In some cases, it can even lead to provisional arrest, or searches and seizures to be followed by a formal request within a specific time.[948]

In addition to a limited use by States,[949] the major flaws of this system are usually related to the training, organisation, and competence of the counterpart[950]. Moreover, the overlapping of multiple contact points in the same country (most European States are part of the Interpol, Europol, G8 and CoE Convention's 24/7 networks), often located within different authorities (e.g. law enforcement agencies or public prosecution offices), may create confusion and delays in the fulfilment of requests.[951]

---

941 CoE, *Convention on Cybercrime* (n 81), Art. 35.

942 *Ibid:* "'24/7' points of contact shall facilitate, or, if permitted by domestic law and practice, directly carry out…".

943 *Ibid.* See also EU, *2005 Framework Decision on attacks against information systems* (n. 82), Article 11: "Exchange of information – 1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week."

944 See CoE, Discussion paper (Prepared by the Economic Crime Division), *The functioning of 24/7 points of contact for cybercrime* (2009), 16.

945 For example, the Interpol networks.

946 See UNODC, *Comprehensive Study on Cybercrime* (n 66), 209.

947 *Id.*, 210.

948 *Idem,* 212. See, e.g., CoE, *Convention on Cybercrime* (n 81), Art. 25.3: "Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication".

949 See UNODC, *Comprehensive Study on Cybercrime* (n 66), 201, 208.

950 See CoE, Discussion paper (Prepared by the Economic Crime Division), *The functioning of 24/7 points of contact for cybercrime* (n 944), 31.

951 See *Id.*, 209-210.

Informal direct cooperation at the investigative level may also be effectuated based on customary practice, diplomatic relations, or private networks between agencies, and be regulated by domestic guidelines or unwritten rules.

At the law enforcement level, international and regional police organisations retain a pivotal role in engendering interstate cooperation and coordination. In particular, the Interpol Digital Crime Center, Europol's European Cybercrime Centre, and the Joint Cybercrime Action Task Force (initiated by Europol's European Cybercrime Centre, the EU Cybercrime Taskforce, the FBI, and the UK's National Crime Agency) are focused explicitly on cooperation against cybercrime.[952]

In order to assist the party in its investigations, proceedings, or promote formal cooperation, some legal assistance mechanisms envisage spontaneous disclosure to foreign authorities of information obtained during investigations.[953] Sharing of information at the investigative level is not dependent on traditional cooperation limits and grounds of refusals (although it remains subject to human rights limits to which the involved States are bound). However, it may be subject to conditions imposed by the transferring authority.[954] Prior to delivering such information, the providing Party may request that it be kept confidential or only used subject to conditions.[955] In particular, limitation to use as evidence in judicial procedures may be requested.

---

[952] As an example of successful interagency operation, in 2015 the FBI and Europol's European Cybercrime Centre coordinated law enforcement agencies from 20 countries in the technical takedown of a prominent criminal Internet forum (Darkode) and in numerous related law enforcement actions resulting in numerous arrests, searches, and seizures. Europol Press Release, 'Cybercriminal Darkode Forum Taken Down through Global Action' (15 July 2015) <https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action>; FBI Press Release, 'Major Computer Hacking Forum Dismantled' (15 July 2015) <https://www.fbi.gov/pittsburgh/press-releases/2015/major-computer-hacking-forum-dismantled>.

[953] See CoE, *Convention on Cybercrime* (n 81), Article 26; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 33. See supra at xxx.

[954] See CoE, *Convention on Cybercrime* (n 81), Article 26.2; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 33.2. Besides the extralegal consequences of their incompliance, when required by an international treaty regulating information sharing, States are under an international duty to fulfil the conditions.

[955] If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

IV.IV.III. EXTRATERRITORIAL ACTIVITIES.

As a general rule, following the principle of State sovereignty over its territory, States cannot exercise extraterritorial enforcement jurisdiction in relation to persons, objects and cyber activities, except on the basis of a specific allocation of authority under international law, or valid consent by the territorial State.

It is commonly agreed that law enforcement officials may access publicly available (open source) stored computer data without the authorisation of another State, regardless of where the data is geographically located.[956] Such access is not considered to constitute either an exercise of enforcement jurisdiction in itself or a violation of another State's sovereignty.[957] This consideration is primarily based on the fact that, since the Uniform Resource Locator (*simpliciter:* web address) does not *per se* indicate the location of the data, during an investigation on the web an infringement of the sovereignty of another State can never be prevented.[958]

Per contra, investigative or coercive measures on cyberspace, even publicly accessible, such as a search or seizure or undercover infiltration of cyber activity, that nonetheless interfere with the territorial State's sovereign prerogatives over cyber infrastructures and activities within its territory, require consent on the part of the territorial State. Lacking such consent, the activity amounts to an unlawful exercise of enforcement jurisdiction and a violation of the territorial State's sovereignty.

In some cases, consent is granted by means of a treaty. Typical examples may be found in agreements allowing for cross border pursuit and infiltration[959] or the setting up of joint investigation teams[960]. With regard to cybercrime, the Directive on the European Investigation

---

956 See M. N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 11, § 12. See also CoE, *Convention on Cybercrime* (n 81), Article 32(a); LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 40.1; Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Section IV, General Report, 19; Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Section IV, Final Resolution, 8 - 9.

957 See N. Seitz, 'Transborder Search:

A New Perspective in Law Enforcement?', (2005) 7 Yale Journal of Law & Technology 23, 6; US, Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002), 25.

958 See N. Seitz, 'Transborder Search:

A New Perspective in Law Enforcement?' (n 957), 6.

959 See, e.g., EU, *Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders*, OJ L 239, 22 September 2000, Articles 40 and 41; CoE, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, ETS 182, 8 November 2001, Article 17.

960 See, e.g., EU, *Council Framework Decision 2002/465/JHA on Joint Investigation Teams*, OJ L 162, 20 June 2002; EU, *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 19 July 2003, Article 5; CoE, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* (n 959), Article 20.

Order introduces the possibility of extraterritorial investigative activity, aimed at the interception of telecommunications. It specifically envisages EIOs being issued for the interception of telecommunications in the Member State from which technical assistance is requested. In cases where the interception of telecommunications involves a "communication address," used on the territory of another Member State – but no technical assistance is needed to carry out the interception – the Directive merely requires the intercepting State to notify the other Party of the interception. It therefore allows extraterritorial interception of telecommunications. The Directive contains limited safeguards against a possible abusive use of such a tool. It provides for the possibility of the territorial State communicating that the interceptions shall not be carried out or shall be terminated and that any material already intercepted while the subject of the interception was on its territory may not be used, (or may be used only under specified conditions).

Furthermore, Article 32(b) CoE Convention on Cybercrime and Article 40.2 LAS Convention on Combating Information Technology Offences provide *a priori* consent for remote extraterritorial cyber investigations.[961] According to these provisions, a party may access or receive stored computer data located in the territory of another Party without its *ad hoc* authorisation, provided it has obtained the lawful and voluntary consent of the person who has the authority to disclose data.

Transborder access to stored data is one of the most discussed and problematic tools of the fight against cybercrime. It has manifest repercussions on the sovereignty of States and, possibly, on the human rights of the suspect/accused.[962]

Transborder access substantially grants the authorities of a Member State the power to "bypass" traditional modes of cooperation and directly compel the physical or legal person who has the lawful authority to disclose data (for instance, the suspect, or ITCs or private entities holding data).[963]

---

961 A. Osula, 'Transborder access and territorial sovereignty', (2015) 31 *Computer Law & Security Review* 719; N. Seitz, 'Transborder Search:
A New Perspective in Law Enforcement?' (n 957), 23; K. Giles, 'Russia's Public Stance on Cyberspace Issues' in C. Czosseck, R. Ottis and K. Ziolkowski (Eds), 2012 4th International Conference on Cyber Conflict (NATO CCD COE Publications, 2012), 67.

962 See CoE, Discussion Paper (Prepared by the Transborder Group), *Transborder access and jurisdiction: What are the options?* (2012); N. Seitz, 'Transborder Search:
A New Perspective in Law Enforcement?' (n 957).

963 See CoE, Discussion Paper (Prepared by the Transborder Group), *Transborder access and jurisdiction: What are the options?* (n 962), 22-23.

The traditional mutual assistance framework is grounded on a bilateral relationship of assistance, usually formalised in a legal instrument, which sets out limits and grounds – also related to the rights of the persons involved – on which the assistance is requested and offered. Transborder access to stored data lies outside such bilateral procedures. Through its investigating powers, the State directly and unilaterally extends the exercise of its enforcement jurisdiction outside its borders, without requesting the assistance of the territorial State.

The main problems related to the use of this tool arise from possible violations of human rights.[964] As alluded to by the CoE Ad-hoc sub-group on jurisdiction and transborder access to data and data flows (Transborder Group), transborder access is outside the scope of the traditional limits of international cooperation – such as the double criminality rule or the political offence exception – which are primarily aimed at protecting the fundamental rights of the suspect/accused.[965] It may thus be used to circumvent such limits. For instance, a State may use transborder access to conduct cross-border searches against political dissidents. Moreover, while searching computer systems located abroad, State authorities may operate under standards and modalities that concretely ignore rights and guarantees provided for in the domestic law of the State, where the system is located, which the suspect/accused reasonably expects to be applied.[966]

This tool therefore needs a narrower regulation, in order to limit possible human rights violations.[967] To avoid misuse, it may be essential to reconcile it with the grounds of refusal provided for by mutual assistance. For instance, the possibility of entrusting the territorial State with the power to revoke *ex post* the consent to a search and, generally, to limit the scope of action of the investigating authorities under a basic regulation, should be envisaged.

---

964 See CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), §293: "The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof".

965 See CoE, Discussion Paper (Prepared by the Transborder Group), *Transborder access and jurisdiction: What are the options?* (n 962), 12.

966 *Idem*, 12-13.

967 It may also need terminological clarification, in particular on who the "person who has the lawful authority to disclose the data" is.

Nevertheless, at least theoretically, the State may intervene at the national level by regulating the providers' authorisation grant to foreign authorities under certain conditions.

IV.IV.IV. COOPERATION BETWEEN STATES AND PRIVATE ENTITIES.

With the growing diffusion of fast Internet connections and cloud storage services, data is rapidly moving from private hardware to data centres owned by ITCs. Presently and at an increasing extent, it is a common practice for law enforcement authorities to request (content or non-content) data from ITCs.[968]

The issue of cooperation between States and ITCs holding data contains two essential jurisdictional aspects: State competence over the provider, and State competence over data itself. The lack of a stable international position on the issue has fostered controversial approaches, which were mainly determined within the internal vertical relation between ITCs and States.

Data collection within criminal investigation shall comply with due legal process. Therefore, States should request data from ITCs subject to their jurisdiction in accordance with their domestic procedural provisions and applicable human rights norms. State jurisdiction on ITCs can be allocated based on a significant connection to the State territory, which may be established through the conduction of activities on that territory. Article 18 of the CoE Convention on cybercrime, for instance, allows production orders to be directly addressed to an ITC "offering its services in the territory" of the State. [969]

Nonetheless, ITCs' guidelines often require foreign States (even those on the territory of which they conduct activities) to demand data through formal cooperation requests, directed to the

---

[968] See e.g. CoE, Cybercrime Convention Committee, *Assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, T-CY(2013)17rev, 3 December 2014, 7. See also transparency reports on law enforcement requests at: https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/; https://www.google.com/transparencyreport/?hl=en-US; http://l.yimg.com/pj/info/tr/Yahoo_Transparency_Report-Jan-June-2013-1.3.pdf https://www.facebook.com/about/government_requests.

[969] See *supra* § III.II.I. See also O. Pollicino and G. Romeo (Eds), *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe* (Routledge 2016), 42-43. This criterion is rather vague and does not find clarification in the Convention nor its Explanatory Report. It was clarified in 2017, by a Guidance Note, which presents a two-folded test: "1) Does the service provider enable persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services)? 2) Has the service provider established a real and substantial connection to a Party?". See P. De Hert, C. Parlar and J. Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law', (2018) 34 Computer Law & Security Report 327.

State of their central seat.[970] Such guidelines reveal a preference for a link based on nationality, which may avoid jurisdictional multiplications.

An example of this came in 2007 when, in the Belgian Yahoo! Case, the Belgian law enforcement agency requested information from the company "Yahoo!" under Article 46bis of the Belgian code of criminal procedure. This provision imposes on providers of electronic communications services[971] an obligation to cooperate with the law enforcement agency. Yahoo! refused direct disclosure and indicated a formal mutual assistance request to US authorities as the proper channel by which to obtain the demanded data.[972] In 2015, the Belgian Court of Cassation found Yahoo! to be under Belgian jurisdiction, thereby confirming the order to hand out the requested data (which, to this day, has never been complied with).[973]

Lacking jurisdictional competence over the ITC, the assistance of the competent State has to be demanded under existing cooperation mechanisms. If data is stored in data centres located outside the State's territory, the assistance of the territorial State or its consent to extraterritorial access to data may be necessary. However, the service provider is often requested to retrieve data from its extraterritorially-located data centres directly and hand it out to the requesting State.[974]

In a case where the ITC directly owns and controls data, or the data owner consents (possibly, through the ITC's Terms and Conditions), it is disputed whether this situation may, at least partially, fall under the scope of the CoE Convention provisions on transborder access with the consent of the person who has the lawful authority to disclose data.[975]

The predominance of a vertical, control-focused approach (meaning direct power by an ITC over data), with reduced importance of the territorial State, is revealed by the widely accepted possibility of ITCs' voluntary data disclosure through specific procedures in case of emergencies, such as a risk of death or serious physical injury to any person.[976] Although openly

---

970 See, e.g., 'Facebook Operational Guidelines for Law Enforcement Authorities' https://www.facebook.com/safety/groups/law/guidelines/).

971 Electronic communications services are services provided by means of electronic signals over, for example, telecommunications or broadcasting networks (see EU, *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services,* OJ L 108, 24.4.2002).

972 See P. de Hert and M. Kopcheva, 'International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case' (2011) 27 Computer Law & Security Review 291; P. de Hert, C. Parlar and J. Thumfart, 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland', (2018) 9 New Journal of European Criminal Law 326.

973 Belgium, Hof van Cassatie van België, *1 December 2015, P.13.2082.N/1.*

974 See US, *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

975 See CoE, Cybercrime Convention Committee, *Guidance Note # 3 Transborder access to data (Article 32)*, T-CY (2013)7 E, 3 December 2014, 7.

976 See, e.g., 'Facebook Operational Guidelines for Law Enforcement Authorities' (n 970).

criticised, these control-focused models should be understood in light of the decreased significance of the territorial link between States and data, which has been eroded by automatic data placements across data centres, or simultaneous placement in multiple data centres, mainly without the owner's or the territorial State's awareness. Furthermore, it is related to the need to avoid complex models of cross-cooperation between the requesting State, the ITC, the State with jurisdictional competence over the ITC, and the State with jurisdictional competence over the relevant data.

In any case, these models do not provide States with direct coercive power over extraterritorial data. In cases of the non-compliance of an ITC with a disclosure request, States may need to request the assistance of the territorial State (or request consent to direct extraterritorial access).

IV.IV.V. LIMITS AND GROUNDS FOR REFUSAL.

Traditional international cooperation in criminal matters is an expression of a mutual relationship between sovereign entities. As such, it is mainly structured around States' interests, and on the principle of respect for State sovereignty. However, the process of mutual cooperation has significant human rights implications. Its dogmatic structure is inherently connected to the human rights of the individuals involved in the cooperation process.

Indeed, mutual cooperation in criminal matters has been historically based on a "bi-dimensional" relation between sovereign States[977]. At one time, cooperation was entirely focused on these States' interests. Procedures were aimed at balancing non-interference in internal affairs, reciprocal diffidence, and the need for close cooperation in crime repression. The persons involved were entitled to the sole rights and safeguards arising from their passive position as the objects of a relation between States[978]. Presently, the injection of human rights into the national and international rules governing interstate cooperation led the persons involved, and their rights, to gain a prominent and active position in the cooperation process.

---

977 See O. Lagodny, *Expert Opinion for the Council of Europe on Questions Concerning Double Criminality*, PC-OC/WP (2004), 3. See also M.C. Bassiouni, 'Human Rights in the Context of Criminal Justice: Identifying International Procedural Protections and Equivalent Protections in National Constitutions', (1993) 3 Duke Journal of Comparative and International Law 235, 240: "Historically, the notion of sovereignty has been a bar to the application of international substantive legal norms to national criminal justice processes".

978 See: S. Williams, 'Human Rights Safeguards and International Cooperation in Extradition: Striking the Balance', (1992) 3 Criminal Law Forum 191, 192.

To a certain extent, mutual cooperation is now a tripartite process, bound to observe both a State's sovereignty and binding human rights obligations. The interests of concerned States and individuals are embodied in various limits defining the boundaries of the obligation to cooperate, either to be found in protective principles internal to the cooperation framework, or in the "external" international law system. More specifically, cooperation is subject to the limits and grounds of refusal provided for by the specific cooperation framework in force between the States in question, to those contained in their national laws, and to the international human rights obligations to which such States are bound.

The first ground for refusal to cooperate arises where cooperation would contravene *ius cogens*. The far-reaching non-derogable duty stemming from peremptory norms implies that States are not bound by an obligation to cooperate where the assistance will likely violate such norms (e.g. the prohibition of torture).

Furthermore, States' duty to cooperate shall be reconciled with other conventional obligations to which a State may be bound. In particular, mutual cooperation in cyber criminal matters shall comply with the applicable human rights obligations to which the States involved are bound. Most international instruments which address interstate cooperation – including the cyber specific instruments analysed here – contain clauses recalling human rights based limits to cooperation. In the EU, such limits are embodied in the EU Treaties[979], and recalled by the CJEU case law.[980]

Particular complexities arise concerning the scope of application of such obligations, since an interstate cooperation process may involve interests of individuals located outside the jurisdiction of the relevant State. Extraterritorial cyber investigations should be regulated by the "agent control standard", in light of which a State, acting outside its jurisdiction and exerting direct authority and control over an individual, must comply with its human rights obligations.[981] Conversely, within the cooperation process, the involvement of the cooperating

---

[979] TEU, Articles 6 and 21(1); TFUE, Article 67(1).

[980] CJEU, *Åklagaren v Åkerberg Fransson* [2013] EUECJ C-617/10, § 45. See also the ECtHR case law: e.g. Coe, European Committee on Crime Problems, Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters, *Case Law by the European Court of Human Rights of Relevance for the Application of the European Conventions on International Co-Operation in Criminal Matters*, PC-OC (2011) 21 REV 12 (2018).

[981] See, inter alia, UN, Human Rights Council, *Lopez Burgos v Uruguay*, *Saldias de Lopez (on behalf of Lopez Burgos) v Uruguay*, Merits, Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979, IHRL 2796 (UNHRC 1981), 29 July 1981; International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion (9 July 2004); ECtHR, *Al-Skeini and Others v. the United Kingdom* (Application n. 55721/07), 7 July 2011; ECtHR, *Issa and Others v. Turkey* (Application n. 31821/96), 16 November of 2004. See also, Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (n 204), Final resolution, § 19.

State in human rights violations by the other State may not rise to the level of being "direct". Nonetheless, according to ample national and international jurisprudence, the mere foreseeability of a substantial risk of prospective human rights violations within the cooperation process may generate a relevant degree of involvement of the cooperating State so as to engage its human rights obligations.[982] The existence of a real risk of human rights violations by the other State shall thus preclude cooperation. In a cooperation process involving cyber investigative activities, the risks of infringement of human rights are typically focused on the right to privacy of the persons involved. On this point, extensive discussion has been had in the previous chapter on procedural law, to which the reader is referred.[983]

The boundaries of State and individual interests within the cooperation process are more clearly defined in the limits and grounds of refusal traditionally embedded in the cooperation framework. Internal protective principles may be found either in the international bases regulating cooperation between the involved parties, or in their domestic system.

The cooperation framework in the existing cyber specific treaties adopts traditional limits to interstate cooperation and grounds for its refusal. The CoE Convention, for instance, expressly recalls the protective principles contained in the domestic law of the parties, and specifically envisages optional grounds for refusal. These include the offence's political character and prejudice to State sovereignty, security, *ordre public* or other essential interests.[984] The far-reaching scope of these latter grounds of refusal should be read in combination with the overall duty of States to cooperate under the agreements, in order to exclude categorical and systematic refusals.[985]

An additional pivotal condition to cooperation is the principle of double criminality, which requires that the crime with respect to which the cooperation is sought be criminalised in both

---

[982] See, inter alia, ECtHR, *Soering v. The United Kingdom* (Application n. 14038/88), 7 July 1989; Human Rights Committee, *Chitat Ng v. Canada*, Communication No. 469/1991, U.N. Doc. CCPR/C/49/D/469/1991 (1994); UN Committee Against Torture, *Chipana v. Venezuela*, 10 November 1998, CAT/C/21/D/110/1998. Se also, H. van der Wilt, 'On the Hierarchy between Extradition and Human Rights', in E. De Wet and J. Vidmar (Eds), *Hierarchy in International Law: The Place of Human Rights* (OUP 2012), 148-175.

[983] See *supra* at III.IV.

[984] CoE, *Convention on Cybercrime* (n 81), Article 27.3; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Article 35. Activation of these limits can theoretically happen in case of cooperation sought for "cyber espionage" made by digital activists or whistle-blowers. For instance, the political nature of the crimes on which the extradition for Julian Assange is sought has been highlighted by some commentators (J. Gerstein, "Dispute over 'political' crimes looms over Assange extradition" (Politico.com, 11 April 2019) <https://www.politico.com/story/2019/04/11/julian-assange-extradition-1271842>).

[985] See, in particular, on the systematic refusal of assistance on data protection grounds, CoE, *Explanatory Report to the Convention on Cybercrime* (n 85), § 269; EU, *Agreement on mutual legal assistance between the European Union and the United States of America*, Article 9.2(b), on condition to providing evidence or information and related explanatory note.

the requesting and requested State. The CoE conventions envisage the principle of double criminality *in abstracto*[986] as an optional ground for refusal to cooperate[987]. This principle appears of particular importance in relation to criminal cyber activities, due to the existing gaps in their criminalisation, as extensively considered in the chapter on substantive law.[988]

---

[986] Double criminality *in abstracto* requires that the act is punishable in both orders, regardless of its *nomen iuris*, even if a State law place the offence within a different category of offence or use different terminology in denominating the offence. In such a case, technical differences and variations in the legal categorisation of a criminal conduct are not hindering cooperation.

[987] CoE, *Convention on Cybercrime* (n 81), Articles 24.1, 25.5, 29.3-4; LAS, *Arab Convention on Combating Information Technology Offences* (n 240), Articles 32.5, 37.3-4.

[988] The "Love Bug" case illustrates the challenges of double criminality. In 2000, the virulent "Love Bug" malware infected millions of private and public computers worldwide, generating billions of dollars in damages. Cooperation between law enforcement agencies worked smoothly and quickly led to the identification of the creator and disseminator of the malware in the Philippine. However, at that time, the Philippine penal legislation did not criminalise virus distribution, nor illegal access to computer systems; moreover, the Philippine cooperation framework envisaged the double criminality principle. Therefore, due to lack of criminalisation of the act in both cooperating parties, extradition to one of the several countries which suffered damages from the malware was disallowed. See *supra* at I.II.II.

V

CONCLUSION

"The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom." [989]

[989] I. Asimov and J. Shulman (Eds), *Isaac Asimov's Book of Science and Nature Quotations* (Weidenfeld & Nicolson 1988), 218.

From electronic circuits, transistors, and microprocessors, to the Internet, smart portable devices, and artificial intelligence; the Digital Revolution has completely changed the world.

Digital technology has become our environment. We live surrounded by it and, at the same time, we also live *in* it. The relationship between human and technology, however, is not merely functional and sterile. We have established a symbiotic relationship with the machine.

The impact of the digital revolution on human society has been vast. It created a "homo digitalis", who expresses his/her life in cyberspace, *with* and *through* new technologies.

Today, the economy and commerce are highly digitalised. Money is dematerialised into a series of 1s and 0s. Roughly 90% of the world's money is digital.[990] Payment systems are embedded in our smartphone. In the second quarter of 2019, the online money transfer provider PayPal processed around 3 billion payments and had 286 million active user accounts worldwide.[991] Finance increasingly relies on digital technologies. At the end of June 2019, there were over 40 million Blockchain wallet users,[992] and 60% of the market value of this technology was concentrated in the financial field.[993] We also sell and buy goods on the web – more than 353 million products are offered online by Amazon.com alone.[994]

Information has also moved into cyberspace. The web, and in particular social media, are becoming the primary source of news for many individuals.[995] At the same time, political institutions are increasingly using such digital tools as their primary means of communication with citizens.[996]

The Internet has drastically changed our social and communication methods and will continue to do so. It has allowed for instant global communication between people, offering new ways of sharing information, data and knowledge. By mid-2018, more than 1.5 billion people worldwide

---

990 See Future Agenda, 'Digital Money' <https://www.futureagenda.org/insight/digital-money>.

991 J. Clement, 'PayPal's net number of payments from 1st quarter 2014 to 2nd quarter 2019 (in millions)' (Statista.com, 26 July 2019) <https://www.statista.com/statistics/218495/paypals-net-number-of-payments-per-quarter/>

992 M. Szmigiera, 'Number of Blockchain wallet users globally 2016-2019' (Statista.com, 7 October 2019), <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/>.

993 S. Liu, 'Blockchain technology market size worldwide 2018-2023' (Statista.com. 9 August 2019), <https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/>.

994 'How Many Products Does Amazon Sell?' (Scapehero, April 2019) <https://www.scrapehero.com/number-of-products-on-amazon-april-2019/>.

995 E. Shearer, 'Social media outpaces print newspapers in the U.S. as a news source' (Pew Research Center, 18 December 2018) <https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/>.

996 See US, *Knight First Amendment Inst. at Columbia Univ. v. Trump*, No. 1:17-cv-5205 (S.D.N.Y.), No. 18-1691 (2d Cir.), holding that US President's practice of blocking critics from his Twitter account violates the First Amendment.

were connected on Whatsapp. These users send some 65 billion messages per day through the mobile app.[997]

The emergence of an open and international space, instantly connecting people from all over the world, has favoured cultural globalisation. In this space, the individual meets, discusses, shares knowledge and information, and receives cultural, ethical and social stimuli.

Digital technology has also become a container for information. We store information in our devices, or in servers we "rent" from ITCs. This information comprises all the aspects of our lives: our finances, our health, our work projects, the messages we share with our loved ones, and so on. According to some analysts, data created, captured, or replicated worldwide in 2018 amounted to 33 zettabytes (33 trillion gigabytes).[998] This number is exponentially growing.

Digital technology is composed of material devices: smartphones, computers, servers, cables, and satellites. Nevertheless, it creates abstract concepts, the description of which often requires the use of metaphors. Of all the metaphors used in this work, the analogy with a "space" seems the most fitting to describe such technology. In this (cyber)space, we place and store information (a repository), we meet people, do business, and share information (an agora), we connect with the world (a road).

Cyberspace is an *alter* (parallel) space. It mimics the physical world in its central social tenets. Many activities are conducted therein, including crime.

In cyberspace, we communicate and store information. Such non-physical information – stored in devices or flowing through the communication process between two machines – is increasingly important in criminal investigations concerning both cybercrimes and ordinary crimes.

Cyberspace is transnational in nature. It is not divided into well-delimited territories, each responding to distinct authorities. A crime committed in cyberspace may reverberate throughout several legal systems and the traces of such crime may therefore be subject to various jurisdictions. Any state action on cyberspace thus depends upon the existence of specific tools of cooperation.

Any response to cybercrime will be ineffective without a transnational minimum level of criminalisation, effective tools of interstate cooperation, and procedural measures suited to the particularities of data.

Several multilateral instruments have been adopted to stimulate the diffusion of a new system of rules able to address the peculiarities of cyber: the technology, the concepts of time and space therein applicable, and the characteristics of data.

---

997 F. Richter, 'WhatsApp Usage Shows No Signs of Slowing Down' (Statista.com, 7 May 2018) <https://www.statista.com/chart/13762/whatsapp-messages-sent-per-day/>.

998 See D. Reinsel, J. Gantz and J. Rydning, *The Digitization of the World From Edge to Core* (IDC White Paper 2018), 3.

In particular, in 2001 a Convention on Cybercrime was adopted under the aegis of the Council of Europe. This convention is presently the most important cybercrime instrument due to its number of ratifications, its geographical diffusion, and the scope of its application. It has worked as a template for most instruments of cybercrime worldwide, including the EU instruments on cyberattacks.

However, the cyber realm is continually evolving, at a pace that is not currently being matched by legislative reform.

V.I. SUBSTANTIVE LAW.

Difficulties in differentiating, selecting, and scaling the punishment for different cyber offences may be natural to cybercrime law. Cybercrimes are inherently broad in scope. They revolve around a technological element that is widely diffused, continually changing, and covering different goods. For instance, the term "computer system" covers both a personal smartphone and national health system's servers. Furthermore, the meaning of the term has changed over time (today, "computer system" means something different than in 2001), and is expanding. Socio-technological evolution (the introduction or diffusion of new technologies; the emergence of new digital-related behaviours)[999] is modifying cybercrime. Many public and private activities have been, or are in the process of being digitalised. Every year, an increasing number of goods become more vulnerable to cybercrime.

The multilateral instruments on cybercrime forecasted such evolution. The solution adopted to address technological changes was to employ technology-neutral language, in the attempt to create a broad scope of application of the provisions on present and future technologies.[1000] This solution bears a significant risk: detaching the offence from the legality, *ultima ratio,* and proportionality principles.[1001] Furthermore, the limits to excessively broad offences have not been specified at the international level. Such limits are to be found in the general principles of criminal law and the human rights of the person involved – and are thus largely left to individual States to determine according to their criminal law systems and human rights obligations.

A comparative analysis of the national substantive cybercrime frameworks reveals a fracture between the law and empirical reality. Discrepancies between the behaviour described in the offence and the actual appearance of the crime may be primarily related to the difficulty of the legislator and the interpreter to understand cyberspace and digital technology fully. In many cases, cyber behaviours are distorted by analogical interpretations. A correct legal perception of the behaviour behind the norm may need (along with a certain degree of technical knowledge) new epistemological tools. The old ideas forged in relation to "physical" criminal law doctrine should be abandoned in favour of a new vision. For instance, rationalisation of the cyber offences within the

---

[999] For instance, when this dissertation was conceived, people (the author is included) were not spending most of their free time staring at their smartphone.

[1000] See § II.II.II

[1001] See § II.II.III.

special part of criminal law may be beneficial. A dedicated space may provide a "sterile lab" to the interpreter and avoid dangerous pairings between cyber behaviours and "similar" traditional crimes. Furthermore, the analysis of the systems involved in the harmonisation process shows significant differences between them. The origin of this problem can be traced back to the international obligation. The essential issue is the lack of attention paid to technological details, and to the precise legal interest to be protected. This failing has been conducive of different approaches to the same offence. An obvious example of this is the offence of illegally accessing a computer system. The interpretations adopted at the domestic level are various. The offence may repress acts of concrete endangerment of the confidentiality, integrity, and availability of computer systems; protect the mere confidentiality of data; or be constructed to protect the property rights of the computer system's owner and his/her *ius excludendi alios*. These differences are far from minor, as they can each lead the scope of the offence being extended over entirely different conducts.[1002]

Furthermore, this work has analysed both the extension of cyber offences over particularly serious conducts (such as terrorist cyberattacks), and over marginal conducts (overcriminalization). Regarding the former, it has been considered whether large scale or terroristic cyberattacks deserve specific regulation.[1003] The analysis here given has evidenced how these acts are usually dealt with as traditional cybercrimes or ordinary offences. Cyberterrorism has received limited autonomous regulation, and the few cyberterrorism provisions enacted have shown a lack of precision in identifying it as a distinctive breed of terrorism deserving a specific approach.[1004]

With regard to the overcriminalisation, the analysis began by evaluating the sociological changes brought about by technological evolution. It considered if the limits to excessively broadened offences have been specified at the international level or, conversely, are mainly left to individual States to determine according to their criminal law systems and human rights obligations.[1005] It then pondered whether certain cyber behaviours should find a place outside the scope of criminalisation, or even be protected by new digital rights. The leading example used has been electronic civil disobedience: a form of online digital protest which, in some cases, could be protected by the right to free expression, assembly, and protest.[1006]

The hacker subculture was instead employed as a case-study to evaluate the social significance of cyberspace (as an *agora* for social aggregation). In particular, *vis à vis* the findings of the social

---

[1002] See § II.III.I.

[1003] See § II.VI.

[1004] See § II.VI.VI.

[1005] See § II.II.IV.

[1006] See § II.V.

sciences with regard to online collective behaviour, this work analysed the application to hacker groups of the substantive provisions constructed to fight traditional collective criminality. Such analysis brought a number of issues to light. Coordination between the members, cohesion within the entity, decentralisation, and amorphic features of the groups are not correctly considered by the norms currently applied, nor by their interpretation.[1007]

This last study uncovered the importance of a fundamental question, running through the whole chapter: to what extent does cybercrime require an original moment of "designation", in which new types of cyber criminal phenomena are analysed through the lenses of social science, and typified in a new criminal offence?

The ultimate diagnosis that emerges from this question is that the existing cybercrime framework suffers from a problem of perception, categorisation, selection of the behaviour, and gradation of the punishment. Inherently different types of behaviour should not be treated in the same way. A terrorist hacking a critical infrastructure and an unauthorised access to a partner's smartphone should not be covered by the same offence.

A remedy may stem from a more in-depth criminological investigation. The more behaviours translate online, and the more activities are conducted in cyberspace, the more understanding of the digital realm is needed. This realm should be organised according to new categories in order to select what should be punished and how. From such a process, we can expect a higher level of precision in defining cyber criminal offences, which will avoid overcriminalisation and "one size fits all" approaches. Criminal laws, and their sanctions, should be based on correct and reliable scientific, empirical, and criminological data.

[1007] See § II.VII.

V.II. PROCEDURAL LAW.

Electronic evidence is increasingly fundamental in trials. This is primarily the case with regard to cybercrime, traces of which exist mainly in electronic form. Due to the growing diffusion of digital technology, electronic evidence has also become highly relevant in ordinary criminal cases. Important information for the process of adjudication may be contained in smartphones, laptops, smart devices, or Information Technology Companies' servers.

Handling electronic evidence is different from handling physical evidence. In particular, data are extremely volatile and very easy to alter, modify, or erase within seconds. These characteristics are to be taken into consideration by specific legal provisions. Some multilateral instruments on cybercrime (but not the EU instruments on cyberattacks) envisage procedural powers aimed at guaranteeing the accuracy and efficacy of cyber investigative operations and avoiding issues related to technical errors, malfunction, or fabrication.[1008]

An additional issue relates to the place where such data are collected. A traditional distinction divides data stored (which may be subject to search and seizure) and data in transit (which may be subject to interception). This distinction, however, is far from definitive. The technology behind data storage and communication is too multifarious to be captured by such a dualistic distinction. Categorisation like this is unable to address data temporarily stored in an ITC or in a server (for instance while an email is "travelling").[1009] This problem is an example of how traditional legal concepts created on physical activities or material goods may fit the digital realm in its complexity. Nevertheless, international instruments have not provided ammunition for further analysis of these issues, which have remained the responsibility of States to resolve.

Furthermore, data is increasingly held by ITCs, rather than being stored in hardware under the direct control of the data owner. In such cases, procedural powers are necessary to obtain data from private parties controlling data. The tripartite relation between individuals, Information Technology Companies, and States is changing. The multilateral instruments envisaged specific procedural tools aimed at provisionally freeze and collect data from ITCs. However, as most ITCs are global enterprises, cybercrime investigations increasingly depend on international cooperation, either with the territorial State in question or with "foreign" private entities.[1010]

[1008] See § III.II.I.

[1009] See § III.II.II.

[1010] See § IV.IV.IV.

Technological evolution has brought significant changes to the investigative panorama. Currently, cyber procedural law faces challenges not considered by the multilateral instruments on cybercrime. On the one hand, the emergence of new technologies – in particular cryptography – has shielded communication from access or interception, substantially hindering investigations. On the other hand, new powerful technologies are at the disposal of the investigative authorities. Extensive gathering of digital evidence is possible with unprecedented ease. Among these technologies, the use of hacking tools is of particular importance, due to its versatility and diffusion. In the lack of a strict principle of procedural legality, such new tools have often been subsumed under existing procedural methods, or have simply found no legal basis.[1011]

In between such technological changes lie the rights of the suspect/accused, in particular their right to privacy. If we continue to fill our digital spaces with personal information (e.g. on our health and financial situation, political and sexual orientation, social contacts), any investigative operation therein conducted may generate unparalleled restrictions of our privacy. This compression of citizens' rights becomes more acute when the tool employed takes full control of one's private cyberspace, acceding to all stored data and intercepting any communication passing from it.

Notwithstanding the increasing attention being paid to privacy in digital technology, the traditional privacy and data protection framework may not be sufficiently specific to address these issues. This is due to the extensive amount of personal information now digitalised (and thus vulnerable) and the increasing power of the cyber investigative tools. A new right to privacy must protect the digital space as an intimate space of the individual – possibly more than other physical spaces. Some legal systems are starting to protect it, granting the individual with a new right to the integrity of his/her digital devices or – more metaphysically – of their "computer domicile".[1012]

[1011] See § III.III.

[1012] See § III.IV.

V.III. JURISDICTION AND INTERNATIONAL COOPERATION.

Let us return to the metaphor we made *supra:* digital technology is a "space", a territory, albeit a virtual one (a cyber-space). This space is composed of a massive amount of data, a library of 0s and 1s that is continually changing and growing. Use of data by humans is largely made possible by a "window", which allows a "passage" into cyberspace (usually a computer, a tablet, a smartphone, or some similar device). A graphic interface translates data into graphics and permits human-machine interaction. The network of online interconnections creates the basic structure of this space, its foundations. These connections create a concrete – yet virtual – space and time dimension.

The rules of time and space in this virtual dimension differ from the standard "physical" concepts on which our laws are based. The time dimension in cyberspace is based on the speed on which data travel. Its space dimension is universal (it covers the whole planet – earth, sea and sky), common (cyberspace is even described by many as a *res communis*, the fifth common space after land, sea, air and outer space), and almost entirely unaffected by the concepts of territory and border in which criminal law has traditionally been rooted.

The spatial nature of digital technology is an intriguing, yet complex concept. Data travel freely across this space (almost)[1013] at the speed of light. We perceive their manifestations on the screens of our devices, yet they travel far, crossing borders and touching servers scattered all over the globe. If this globetrotting is not disconcerting for the user, it may complicate the application of substantive and procedural criminal law. Where is the *locus commissi delicti*? What State has jurisdiction over the crime? Where is the relevant data located? To whom do requests for investigative assistance have to be addressed? The application of the traditional Westphalian conceptions of jurisdiction and interstate cooperation may not provide a precise answer to these questions.[1014]

These problems do not only derive from the peculiar spatial characteristics of cyberspace. They are also related to how data are structured and controlled at the public and private levels. Data is becoming more and more detached from the territory and direct control of States. Investigative authorities may ignore the exact location of the data sought in an investigation. They may try to access them directly, in cyberspace. Eventually, they may have to address their request to private

---

[1013] See 2015 F. Toomey, 'Data, The Speed Of Light And You' (Techcrunch, 8 November 2015) <https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/>.

[1014] See § IV.II.

entities holding data in their data centres. To a certain extent, these entities are now provided with a quasi-subjectivity in the international criminal cooperation system.[1015]

Multilateral cybercrime instruments have addressed these issues. However, these instruments have not promoted any extensive reform of the traditional principles of jurisdiction or the methods of interstate cooperation.

With regard to international cooperation, the multilateral instruments on cybercrime have recognised that the traditional tools of mutual assistance appear to be excessively time consuming and unable to satisfy current investigative needs. In order to provide "increased, rapid and well-functioning international co-operation in criminal matters"[1016], these instruments have introduced a series of specific tools aimed at a quick and efficient investigative response. Most of these tools substantially mirror the solutions contained in the procedural part of the instrument.[1017] In some cases, the multilateral instruments on cybercrime have envisaged the possibility to direct access to data, bypassing the need for the cooperation of the territorial State.[1018]

The latter solutions (transborder access in particular) necessarily encompass an unrestrained interference with the territorial State. They lessen the procedural safeguards provided for by the traditional interstate cooperation tools and generate a risk of violations of the fundamental rights of the accused. Furthermore, they leave individuals at the mercy of foreign States, whose standard of respect of such rights may be questionable. It is hope that such a loss of territorial sovereignty is conceivable solely between States that share a political and legal vision. At the broad international level, such agreements are unlikely to be possible, due to the high level of distrust between States. These tools are freed from a bilateral conception of mutual assistance in criminal matters. Their broad scope is, to some extent, indicative of an approach to cyberspace as a territory that is (partially) independent from the State in which its physical "manifestations" are located. Transnational cooperation in cybercrime cases is melting its structures into cyberspace, following the roads that this metaphysical space has created. The risk is for the individual, and its rights, to be sidestepped. Paradoxically, his/her interests are increasingly protected by ITCs, which are rising as a new subject of the international (cyber) system.

[1015] See § IV.IV.IV.

[1016] CoE, *Convention on Cybercrime* (n 81), Preamble § 8.

[1017] See § IV.IV.I-II.

[1018] See § IV.IV.III.

V.IV. A NEW CONVENTION ON CYBERCRIME?

With a single click of a mouse, a cybercrime can be committed from everywhere towards hundreds of different countries. The repression of such crimes requires efficient interstate cooperation, a common response based on a minimum standard of criminalisation, and the diffusion of cyber-specific procedural tools. If perpetrators are located in a country that does not criminalise a particular type of cybercrime, he/she will most likely enjoy impunity due to the lack of substantive bases to prosecute. This lack reverberates on the effectiveness of interstate cooperation, incapacitated by the "double criminality" principle. Furthermore, the inability to use or request the use of cyber specific procedural powers from the territorial State may seriously hinder investigations. Flaws in legislation may translate into impunity for offenders, inability of the State to satisfy the demand of retribution and specific deterrence, and, in general, ineffective prosecution of crime.

In the past, developing and developed countries have given a differing level of importance to cybercrime. Western societies have always been highly dependent on new technologies. Over time, this dependence has made those countries much more vulnerable to cybercrime, and the main stakeholder in the need for efficient interstate cooperation and broad harmonisation of cybercrime legislation. Developing countries have not so heavily relied on information and communication technology. They have therefore been less affected by cybercrime, and naturally give less attention to the problem, including from a legislative point of view. Along with the political issues related to specific crimes and cooperation tools[1019], this diversity has frustrated the enactment of a comprehensive international instrument on cybercrime.

The harmonisation process is presently fragmented into regional blocks. A significant number of soft laws back several regional legislations. Most of these laws are worryingly outdated and therefore inadequate to satisfyingly cover cybercrime in its current incarnation. Many technical developments are left outside of the scope of the existing legal framework. Numerous issues are not sufficiently

---

[1019] Certain substantive issues – such as political espionage, or right to protest via digital technology – are necessarily contaminated with political considerations. There, an international convention on cybercrime may risk having the same problems perceived in the attempted adoption of an international convention on terrorism. Efforts to reach a consensus may also be frustrated by cooperation issues. Some existing instruments appear to infringe on the national sovereignty and the human rights of the suspect/accused. For instance, permission to unilaterally access computer data stored abroad (with the consent of the person who has the lawful authority to disclose data, and without obtaining permission from the territorial state), as provided in Article 32(b) of the CoE Convention, may be considered one of the main reasons Russia refused to ratify the treaty (Computer Crime Research Center, 'Putin defies Convention on Cybercrime' (28 March 2008) <http://www.crime-research.org/news/28.03.2008/3277/>).

regulated or, in the worst cases, are completely ignored. States are often left with no guidance and are compelled to take autonomous decisions on new criminal behaviours and on new investigative or cooperative challenges.

The Budapest Convention is the only convention on cybercrime with an international scope. It was open to ratification by States non-party to the Council of Europe and currently has acquired a quasi-international dimension. However, it was drafted at the end of the second millennium and, to a large extent, can be considered obsolete.

A new comprehensive treaty may be needed. From a substantive point of view, it is important to have specific regulations around cyberterrorism, cyber-association crimes, and large scale cyberattacks. At the same time, the list of crimes should be based on a behavioural selection able to distinguish between inherently different criminal conducts, while excluding marginal ones.

Balancing human rights protection and the criminalisation of cybercrime can be particularly challenging. Specific attention must be paid to freedom of expression and the right to privacy, which play a pivotal role in the fight against cybercrime. Depending on whether one harbours a more liberal or a more constrained view of these rights, the scope for criminal law enforcement will correspondingly reduce or expand. Individual rights do not enjoy uniform international standardisation. Differences between national approaches may represent a hindrance to reaching a consensus over any future international convention. Even within the Council of Europe, divergence on the balance between freedom of expression and the criminalisation of the distribution of racist propaganda has hindered the inclusion of such a crime in the CoE Convention.[1020]

A paradigm shift is necessary. Any new act of legislation must challenge and eventually abandon the traditional concepts of criminal law that not fit digital technologies. It must recognise the social and anthropological significance of digital technologies, and the related emergence of new digital rights. At the same time, it must understand the international cyber system and the actors within it, acknowledging the increasing role of ITCs. As the technological evolution gives private entities control over most data, the behaviour of these entities and their cooperation with States must be regulated at the international level.

[1020] According to the Explanatory Report to the Additional Protocol: "(t)he committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime". See CoE, *Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime*, ETS 189, 28 January 2003, § 4.

Digital technologies have connected the world. Where States have failed, they have created a common international space. It may be time to provide this space with a comprehensive international regulation.

BIBLIOGRAPHY

* Abadinsky H., *Organized Crime* (Wadsworth Publishing 2010)
* Abelson H. *et al*, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (Columbia University Academic Commons 1997)
* Acquisti A., di Vimercati S. and Grtizaliset S. (Eds), *Digital privacy: theory, technologies, and practices* (CRC Press 2007)
* Akamai, *State of the Internet Security Q4 2015 Report* (Akamai, 2016) <https://www.akamai.com/us/en/multimedia/documents/report/q4-2015-state-of-the-internet-security-report.pdf>
* Albanese, J. S. *Organized Crime in America* (Anderson Publishing 1989)
* Albini J. L., *The American mafia: Genesis of a legend* (Appleton-Century-Crofts 1971)
* AlDairi A., 'Cyber Security Attacks on Smart Cities and Associated Mobile Technologies' (2017) Procedia Computer Science 1086
* Ambos K., 'Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections', (2005) 12 Maastricht journal of European and comparative law 173
* Ambos K., *Treatise on International Criminal Law: Volume 1: Foundations and General Part* (OUP 2013)
* Arquilla J. and Ronfeldt D., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Rand Corporation 2001)
* Article 19, *The "Right to Protest": Background paper* <https://right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf>
* Ashworth A., *Principles of Criminal Law* (OUP 1999)
* Asimov I. And Shulman J. (Eds), *Isaac Asimov's Book of Science and Nature Quotations* (Weidenfeld & Nicolson 1988).
* Association Internationale de Droit Pénal, *XIXème Congrès International de Droit Pénal, La société de l'information et le droit pénal* (2012-2014).
* August R., 'International Cyber-jurisdiction: A Comparative Analysis', (2002) 39 American Business Law Journal 531
* Baauw P., 'Non bis in idem', in Swart B. and Klip A., *International Criminal Law in The Netherlands* (Edition Iuscrim 1997)
* Bainbridge D. I., 'Hacking - The Unauthorised Access of Computer Systems: The Legal Implications' (1989) 52 The Modern Law Review 240

* Baker G. D., 'Trespassers Will Be Prosecuted: Computer Crime in the 1990s' (1993-1994) 12 J. Marshall J. Computer & Info. L. 61
* Barlow J. P., 'A Declaration of the Independence of Cyberspace', in P. Ludlow (Ed), Crypto Anarchy, Cyberstates, and Pirate Utopias (MIT Press 2001)
* Bassiouni M. C. (Ed), *International Criminal Law: Multilateral and Bilateral Enforcement Mechanism* (Martinus Nijhoff Publishers 2008)
* Bassiouni M. C., 'Human Rights in the Context of Criminal Justice: Identifying International Procedural Protections and Equivalent Protections in National Constitutions', (1993) 3 Duke Journal of Comparative and International Law 235
* Bassiouni M. C., *International Criminal Law: Multilateral and Bilateral Enforcement Mechanisms, Volume 2* (BRILL 2008)
* Bassiouni M. C., *International Extradition: United States Law and Practice* (OUP 2014)
* Baudrillard J., *L'echange symbolique et la mort* (Gallimard 1976)
* Baudrillard J., *Simulacra and Simulations* (Éditions Galilée 1981)
* Beirne P. and Messerschmidt J. W., *Criminology* (OUP 2006)
* Bell C. M., 'Surveillance Technology and Graymail in Domestic Criminal Prosecutions', (2018) 16 Georgetown Journal of Law & Public Policy 537
* Bellovin S. M., Blaze M., Clark S. and Landau S., 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet', (2013) 12 Northwestern Journal of Technology and Intellectual Property 1
* Benedek W. and Kettemann M. C., *Freedom of expression and the Internet* (Council of Europe 2014)
* Bengtsson S., 'Virtual Nation Branding: the Swedish Embassy in Second Life', (2011) 4 Journal of Virtual Worlds Research 1
* Bequai A., *Computer Crime* (Lexington 1978)
* Bertram S. K., 'Authority and Hierarchy within Anonymous Internet Relay Chat Networks', (2015) 6 Journal of Terrorism Research 1
* Beyer J. L., *Expect Us: Online Communities and Political Mobilization* (OUP 2014)
* Biasiotti M. A., Mifsud Bonnici J. P., Cannataci J. and Turc F., *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018)
* Blakey G. R. and Gettings B., 'Racketeer Influenced and Corrupt Organizations (RICO): Basic Concepts – Criminal and Civil Remedies', (1980) 53 Temple Law Quarterly 1009
* Blatterer H., Johnson P. and Markus M. R., *Modern Privacy Shifting Boundaries, New Forms* (Palgrave MacMillian 2010)
* Blomsma J., *Mens rea and defences in European criminal law* (Intersentia 2012)

* Bobbit P., *Terror and Consent* (Alfred A. Knopp 2008)
* Bode K., 'UK May Have Finally Ditched Its Absurd Porn Filter Plan' (Techdirt, 21 June 2019) <https://www.techdirt.com/articles/20190620/08544442436/uk-may-have-finally-ditched-absurd-porn-filter-plan.shtml>
* Boister N., "'Transnational criminal law'?" (2003) 14 European Journal of International Law 953
* Brenner S. and Clarke L. L., 'Distributed Security: A New Model of Law Enforcement', (2005) 23 John Marshall Journal of Computer & Information Law 659
* Brenner S. W. and Koops B. J., 'Approaches to Cybercrime Jurisdiction', (2004) 4 Journal of High Technology Law 1
* Brown A., 'This is how much your smartphone knows about you right now' (Express, 7 May 2016)
* Brown I., 'Will NSA revelations lead to the Balkanisation of the Internet?' (The Guardian, 1 November 2013) <http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet>
* Brown S. D., 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2019) ERA Forum
* Bussolati N., 'Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo dell'abusività' (2018) 4 Studium Iuris 428.
* Bussolati N., 'The Rise of Non-State Actors in Cyberwarfare', in Finkelstein C., David Ohlin J. and Govern K. (Eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015)
* Caeiro P., 'The relationship between European and international criminal law (and the absent(?) third)', Mitsilegas V., Bergström M. and Konstadinides T. (Eds), *Research Handbook on EU Criminal Law* (Edwar Elgar 2016)
* Calderoni F., 'The European legal framework on cybercrime: striving for an effective implementation', (2010) 54 Crime, Law and Social Change 339
* Calderoni F., *Organized Crime Legislation in the European Union* (Springer 2010)
* Cangemi D., 'Procedural law provisions of the Council of Europe Convention on cybercrime' (2004) 18 International Review of Law, Computers & Technology 165
* Carter H., 'England riots: pair jailed for four years for using Facebook to incite disorder' (The Guardian, 16 August 2011) <https://www.theguardian.com/uk/2011/aug/16/uk-riots-four-years-disorder-facebook>)
* Cassese A. and Gaeta P., *Cassese's International Criminal Law* (OUP 2013)
* Centers J., *iOS 9: A Take Control Crash Course* (Take Control Books 2015)
* Chan E., 'The Great Firewall of China' (Bloomberg, 6 November 2018) <https://www.bloomberg.com/quicktake/great-firewall-of-china>

* Chanteret C., *Le crime des association de malfaiteurs* (Waltener et Cie 1912)
* Cheng B., "United Nations Resolutions on Outer Space: 'Instant' International Customary Law?" (1965) 5 Indian Journal of International Law 23
* Choo K. R., 'Organised crime groups in cyberspace: a typology', (2008) 11 Trends in organized crime 270
* Clayton R., *Complexities in Criminalising Denial of Service Attacks* (February 2006) <http://www.cl.cam.ac.uk/~rnc1/complexity.pdf>
* Clement J., 'PayPal's net number of payments from 1st quarter 2014 to 2nd quarter 2019 (in millions)' (Statista.com, 26 July 2019) <https://www.statista.com/statistics/218495/paypals-net-number-of-payments-per-quarter/>
* Clementi M., *Storia delle Brigate Rosse* (Odradek, 2007)
* CoE, *Discussion Paper (prepared by H. W. K. Kaspersen), Cybercrime and Internet Jurisdiction* (2009)
* CoE, Discussion paper (prepared by P. Verdelho), *The effectiveness of international co-operation against cybercrime: examples of good practice* (2008)
* CoE, Discussion Paper (Prepared by Research Centre on IT and Law), *Cloud computing and its implications on data protection* (2010)
* CoE, Discussion paper (Prepared by the Economic Crime Division), *The functioning of 24/7 points of contact for cybercrime* (2009)
* CoE, Discussion Paper (Prepared by the Transborder Group), *Transborder access and jurisdiction: What are the options?* (2012)
* CoE, European Committee on Crime Problems, *Extraterritorial Criminal Jurisdiction* (1990)
* Coleman G., *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous* (Verso 2014)
* Collin B., 'The Future of Cyberterrorism: The Physical and Virtual Worlds Converge', (1997) 13 Crime & Justice International Journal 15
* Comey J. B., 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (FBI, 16 October 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>
* Computer Crime Research Center, 'Putin defies Convention on Cybercrime' (28 March 2008) <http://www.crime-research.org/news/28.03.2008/3277/>
* Condliffe J., "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks" (MIT Technology review, 22 December 2016), <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/>
* Conklin J. E., *Criminology* (Pearson 2007)

* Crime Forum Legal Subgroup, *Reform of the Computer Misuse Act 1990* (April 2003) <http://www.internetcrimeforum.org.uk/cma-icf.pdf>
* Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Autonomedia & Critical Art Ensemble 1996)
* Croze H., 'L'apport du droit pénal à la théorie générale de l'informatique (à propos de la loi n 88-19 du 5 janvier 1988 relative à la fraude informatique)', (1988) La Semaine Juridique Edition Générale 18
* Currie R. J. and Rikhof J., *International & Transnational Criminal Law* (Irwin Law 2010)
* D'amato A., 'Can/Should Computers Replace Judges?' (1977) 1 Georgia Law Review 1277
* Daniele M., "La prova digitale nel processo penale", (2011) 66 Rivista di Diritto Processuale 283
* de Certeau M., *L'Invention du Quotidien* (Gallimard, 1980)
* De Francesco G., '*Gli artt. 416, 416 bis, 416 ter, 417, 418 c.p.*', in Corso P., Insolera G. and Stortoni L. (Eds), *Mafia e criminalità organizzata* (UTET 1995)
* de Hert P. and Kopcheva M., 'International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case' (2011) 27 Computer Law & Security Review 291
* de Hert P., 'EU criminal law and fundamental rights', in Mitsilegas V., Bergström M. and T. Konstadinides (Eds), *Research Handbook on EU Criminal Law* (Edwar Elgar 2016)
* de Hert P., 'Identity management of e-ID, privacy and security in Europe. A human rights view', (2008) 13 Information security technical report 71
* de Hert P., González Fuster G. and Koops B., 'Fighting cybercrime in the two Europes. The added value of the EU Framework Decision and the Council of Europe Convention' (2006) 77 Revue Internationale de Droit Pénal 503
* de Hert P., Parlar C. and Sajfert J., 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law', (2018) 34 Computer Law & Security Report 327
* de Hert P., Parlar C. and Thumfart J., 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland', (2018) 9 New Journal of European Criminal Law 326
* De la Cuesta-Arzamendi J. L., 'Tratamiento de la delincuencia organizada en España: en particular, tras la reforma penal del 2010', (2013) 55 Revista Criminalidad 81
* De Otaola Zamora J. and Letai Weissenberg P., *Cyber Law in Spain* (Kluwer Law International 2011)

* de Souza e Silva A., 'From Cyber to Hybrid Mobile Technologies as Interfaces of Hybrid Spaces' (2006) 9 Space and Culture 261
* Delmas Marty M. and Spencer J. R., *European Criminal Procedures* (CUP 2006)
* Desjardins J., 'Why Hackers Hack: Motives Behind Cyberattacks' (Visual Capitalist, 3 January 2018) <https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/>
* Deutsch M. and Gerard H. B., 'A study of normative and informational social influences upon individual judgment' (1955) 51 The journal of abnormal and social psychology 629
* Diani M., 'Leaders or brokers? Positions and influence in Social Movement Networks', in Diani M. and McAdam D., *Social movements and networks: Relational approaches to collective action* (OUP 2003)
* Dibbell J., 'A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society', (1994) Annual Survey of American law 471
* Diefenbach T. and Sillince J. A., 'Formal and informal hierarchy in different types of organization', (2011) 32 Organization Studies 1515
* Diffie W. and Landau S., *Privacy on the line: the politics of wiretapping and encryption* (MIT Press 2017)
* Dishman C., 'The Leaderless Nexus: When Crime and Terror Converge', (2005) 28 Studies in Conflict & Terrorism 237
* Dixon P. (Ed), *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (ABC Clio 2016)
* Dominguez R., 'Electronic Civil Disobedience: Inventing the Future of Online Agitprop Theater' (2009) PMLA 1806
* Dresner E. and Herring S. C., 'Functions of the nonverbal in CMC: Emoticons and illocutionary force', (2010) 20 Communication theory 249
* Dubber M. D., 'Comparative Criminal Law', in Reimann M. and Zimmermann R. (Eds), *Oxford Handbook of Comparative Law* (OUP 2008)
* Dubber M. D., "Criminalizing Complicity A Comparative Analysis" (2007) 5 Journal of International Criminal Justice 977
* Edwards L., 'Dawn of the death of distributed denial of service: How to kill zombies' (2006) 24 Cardozo Arts & Entratainment Law Journal 23
* Electronic Frontier Australia, "Telecommunications Interception Legislation Amendment Bill 2002" <https://www.efa.org.au/Issues/Privacy/tia_bill2002.html#existing>
* Electronic Frontier Foundation, 'Vulnerabilities Equities Process' (EFF, 2016) <https://www.eff.org/it/document/vulnerabilities-equities-process-january-2016>
* Elliott C., *French Criminal Law* (Routledge 2001)

* Engebretson P., *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (Elsevier 2013)
* EU, European Data Protection Supervisor, *Dissemination and use of intrusive surveillance technologies, Opinion 8/2015*, 15 December 2015
* Europol Press Release, 'Cybercriminal Darkode Forum Taken Down through Global Action' (15 July 2015) <https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action>
* Europol, '24/7 Operational Centre' <https://www.europol.europa.eu/content/page/operational-centre-1853>
* Evron G., 'Battling Botnets and Online Mobs Estonia's Defense Efforts during the Internet War' (2008) 9 Georgetown Journal of Intional Affaires 121
* Fabbrini F., 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States', (2015) 28 Harvard Human Rights Journal 65
* Fafinski S., 'Computer misuse: The implications of the Police and Justice Act 2006' (2008) 72 The Journal of Criminal Law 1
* Falcone D. N., *Dictionary of American criminal justice, criminology, and criminal law* (Pearson/Prentice Hall 2005)
* FBI Press Release, 'Major Computer Hacking Forum Dismantled' (15 July 2015) <https://www.fbi.gov/pittsburgh/press-releases/2015/major-computer-hacking-forum-dismantled>
* Feldman D., 'Secrecy, dignity, or autonomy? Views of privacy as a civil liberty', 47 Current Legal Problems 41
* Fijnaut C. and Paoli L. (Eds), *Organized Crime in Europe* (Springer 2006)
* Finckenauer J. O., 'Problems of definition: what is organized crime?' (2005) 8 Trends in organized crime 63
* Finklea K., *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations* (Congressional Research Service 2016)
* Fischer T., "§ 129, Bildung krimineller Vereinigungen", in *Strafgesetzbuch und Nebengesetze* (Beck 2012)
* Fletcher G., 'The Indefinable Concept of Terrorism', (2006) 4 Journal of International Criminal Justice 894
* Fletcher G., *Basic Concepts of Comparative Law* (OUP, 1998)
* Flor R., 'Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios' (2005) 1 Diritto Penale e Processo 85

* Franzese P. W., 'Sovereignty in Cyberspace: Can it exist?', (2009) 64 Air Force Law Review 1
* French P., *Collective and Corporate Responsibility* (Columbia University Press 1989)
* Future Agenda, 'Digital Money' <https://www.futureagenda.org/insight/digital-money>
* Gana S. H. Jr., 'Prosecution of Cyber Crimes through Appropriate Cyber Legislation in the Republic of the Philippines', <http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html>
* Gercke M. and Brunst P. W., *Praxishandbuch Internetstrafrecht* (W. Kohlhammer Verlag 2009)
* Gercke M., 'Hard and Soft Law Options in Response to Cybercrime: how to Weave a More Effective Net of Global Responses', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)
* Gershgorn D., 'Software Used to Predict Crime Can Now Be Scoured for Bias' (Defence One, 23 March 2017) <http://www.defenseone.com/technology/2017/03/software-used-predict-crime-can-now-be-scoured-bias/136426/>
* Gerstein J., "Dispute over 'political' crimes looms over Assange extradition" (Politico.com, 11 April 2019) <https://www.politico.com/story/2019/04/11/julian-assange-extradition-1271842>
* Gibson W., *Neuromancer* (Ace 1984)
* Giles K., 'Russia's Public Stance on Cyberspace Issues' in Czosseck C., Ottis R. and Ziolkowski K. (Eds), 2012 4th International Conference on Cyber Conflict (NATO CCD COE Publications, 2012)
* Glynn E. A., 'Computer Abuse: The Emerging Crime and the Need for Legislation' (1983) 12 Fordham Urban Law Journal 173
* Goldstein E., 'The Constitution of a Hacker' (1984) 2600 The Hacker Quarterly
* Goodman M. D. and Brenner S. W., 'The Emerging Consensus on Criminal Conducts in Cyberspace' (2002) 10 IJLIT 139
* Goodman M., 'International Dimensions of Cybercrime', in Ghosh S. and Turrini E. (Eds), *Cybercrimes: A Multidisciplinary Analysis* (Springer 2010)
* Gozzi R. J., 'The cyberspace metaphor' (1994) 51 ETC: A Review of General Semantics 218
* Granger M. P. and Irion K., "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection", (2014) 39 European Law Review 835
* Gregory F., 'Private Criminality as a Matter of International Concern', in Sheptycki J. W. E. (Ed) *Issues in Transnational Policing* (Routledge 2000)
* Gregory M. A. and Glance D. (Eds), *Security and the Networked Society* (Springer 2013)

* Groenhuijsen M.S. and Wiemans F.P.E., *Van electriciteit naar computercriminaliteit* (Gouda Quint 1989)
* Gröning L., 'A Criminal Justice System or a System Deficit? Notes on the System Structure of the EU Criminal Law', (2010) 18 European Journal of Crime, Criminal Law and Criminal Justice 115
* Grosso C. F., 'La non punibilità per particolare tenuità del fatto' (2015) 5 Diritto Penale e Processo 1
* Guardian (the), The NSA Files <https://www.theguardian.com/us-news/the-nsa-files>
* Guerrier C., "La révision du code de procédure pénale de 2016: le nouveau régime des interceptions électroniques", (2016) Juriscom.net: droit des technologies de l'information
* Hald S. L. N. and Pedersen J. M., 'An updated taxonomy for characterising hackers according to their threat properties', in *14th International Conference on Advanced Communication Technology* (IEEE 2012)
* Hardy K. and Williams G., 'What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism' in Chen T., Jarvis L., Macdonald S. (Eds), *Cyberterrorism* (Springer 2014)
* Harley B., 'A global convention on cybercrime?' (2010) Columbia Science and Technology Law Review 11
* Hatmaker T., 'Russia plans to test a kill switch that disconnects the country from the Internet' (Techcrunch, 12 February 2019) <https://techcrunch.com/2019/02/11/russia-internet-turn-off-digital-economy-national-program/?utm_source=tcfbpage&sr_share=facebook&fbclid=IwAR0m6sbxmOyH7MJis0PF81vi4YBTgA0L-bad5xq42NOh6ZolOviniVixOkQ>
* Hauben M., 'Behind the Net: The Untold History of the ARPANET and Computer Science', in Hauben M.and Hauben R., *Netizens: On the History and Impact of Usenet and the Internet* (Wiley 1998)
* Hayashi M., 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace', (2006) 6 In Law 284
* Hayashi M., 'The Information Revolution and the Rules of Jurisdiction in Public International Law', in Dunn Caventy M. et al. (eds), *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Routledge 2007)
* Hilgendorf E., '§ 202a Ausspähen von Daten', in *Leipziger Kommentar* (De Gruyter 2010)
* Hoefnagels G. P. (Ed), *The Other Side of Criminology: An Inversion of the Concept of Crime* (Springer Science & Business Media 2013)
* Hoffman A., *Hacking Ma Bell: The First Hacker Newsletter – Youth International Party Line, The First Three Years* (Warcry Communications 2010)

* Hollinger R. C. and Lanza–Kaduce L., 'The process of criminalization: The case of computer crime laws' (1988) 26 Criminology, 101
* Hollinger R. C., 'Computer hackers follow a Guttman-like progression' (1988) 72 Sociology and Social Research 199
* Holt T. J., 'The Attack Dynamics of Political and Religiously Motivated Hackers', in *Proceedings of the Cyber Infrastructure Protection Conference* (City University of New York 2009)
* Hornle J., 'The Jurisdictional Challenge of the Internet', in Edwards L. and Waelde C. (Eds), *Law and Internet* (Hart 2009)
* Hvistendahl M., "Can 'predictive policing' prevent crime before it happens?" (28 September 2016, Science) <http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens>
* Hyman P., 'Cybercrime: It's Serious, But Exactly How Serious?' (Communications of the ACM, March 2013) <http://cacm.acm.org/magazines/2013/3/161196-cybercrime-its-serious-but-exactly-how-serious/fulltext>
* *Imperva's Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack* (Imperva 2012)
* International Conference on the Alternative Use of Computer, *Final Declaration*, <https://n-1.cc/bookmarks/view/1663318/galactic-hacker-party-and-icata89-in-amsterdam>
* Internet Engineering Task Force, *RFC (Internet Security Glossary)* 2828 <https://tools.ietf.org/html/rfc4949>
* Interpol, 'Facial Recognition' (Interpol.int), <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition>
* Interpol, 'Fact Sheet, Connecting police: I-24/7', COM/FS/2011-02/GI-03 (2001)
* Interpol, *Third INTERPOL Symposium on International Fraud*, 11-13 December 1979, Presentation by S. Schjolberg
* ITU, 'Statistics' <https://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx>
* ITU, *Establishment of Harmonized Policies for the ICT Market in the ACP Countries, Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts* (ITU 2012)
* ITU, *Understanding Cybercrime: Phenomena, Challanges and Legal Response* (ITU 2012)
* Jackson P. C., *Introduction to artificial intelligence* (Courier Dover Publications 2019)
* Jacob M., 'Facial recognition gains grounds in Europe, among big-brother fears' (Euroactive, 20 October 2017), <https://www.euractiv.com/section/data-protection/news/facial-recognition-gains-grounds-in-europe-among-big-brother-fears/>
* Jaishankar K., 'Victimization in the Cyberspace: Patterns and Trends', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)

* Jakobs G., 'Die kunkurrentz', in *Strafrecht, allgemeiner Teil: die Grundlagen und die Zurechnungslehre* (De Gruyter 1993)
* Jakobs G., Kriminalisierung im Vorfeld einer Rechtsgutsverletzung', in *Zeitschrift für die gesamte Strafrechtswissenschaft* (De Gruyter 1985)
* Jerker D. and Svantesson B., 'Borders On, or Borders Around—The Future of the Internet', (2006) 16 Albany Law Journal of Science and Technology 343
* Johnson D. R. and Post D., 'Law and Borders -The Rise of Law in Cyberspace', (1996) 48 Stanford Law Review 1367
* Jouvenal J., 'Is crime prediction software the way forward for modern policing? Or biased against minorities?' (The Independent, 22 November 2016) <http://www.independent.co.uk/news/world/americas/crime-prediction-software-modern-policing-or-biased-against-minorities-us-police-law-a7429676.html>
* Kantardzic M., *Data Mining: Concepts, Models, Methods, and Algorithms* (John Wiley & Sons 2019)
* Karanasiou A. P., 'The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks' (2014) 28 International Review of Law, Computers & Technology 98
* Karstedt S., Loader I. and Strang H., *Emotions, crime and justice* (Hart 2011)
* Kehl D., Wilson A. and Bankston K., *Doomed to repeat history? Lessons from the Crypto Wars of the 1990s* (Open technology institute 2015)
* Kerr D., 'Anonymous petitions U.S. to see DDoS attacks as legal protest' (CNet, 9 January 2013) <http://www.cnet.com/news/anonymous-petitions-u-s-to-see-ddos-attacks-as-legal-protest/>
* Kerr O. S., 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes' (2003) 78 New York University Law Review 1596
* Kerr O. S., 'Search Warrants in an Era of Electronic Evidence', (2005) 75 Mississippi Law Journal 85
* Kerr O. S., *Searching and seizing computers and obtaining electronic evidence in criminal investigations* (Office of Legal Education, Executive Office for United States Attorneys 2001)
* Kiesler S., Siegel J. and McGuire T. W., 'Social Psychological Aspects of Computer-Mediated Communication', (1984) 39 American psychologist 1123
* Kirchner J., 'Hackers steal legislators' attention' (ComputerWorld 12 September 1983) <http://www.computerworld.com/article/2523544/government-it/hackers-steal-legislators--attention.html>
* Kirwan G. and Powe A., *Cybercrime: The Psychology of Online Offenders* (CUP 2013)
* Klang M., Murray A. (Ed), *Human Rights in the Digital Age*, (Routledge 2005)

* Klip A. (Ed), *Substantive Criminal Law of the European Union* (Maklu, 2011)
* Klip A. and Van der Wilt H. (Eds), *Harmonisation and harmonising measures in criminal law* (Royal Dutch Academy of Sciences 2002)
* Klip A., *European Criminal Law: an Integrative Approach* (Intersentia 2009)
* Kluitenberg E., Sassen S., Rheingold H., Brams K., Pultau D., *Open 11: Hybrid Space* (Nai Uitgevers Pub 2006)
* Kohls S. J., 'Searching the Clouds: Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account' (2012) 4 Case Western Reserve Journal of Law, Technology & the Internet 169
* Koops B. J. and Goodwin M., 'Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law' (Tilburg Institute for Law, Technology, and Society and Center for Transboundary Legal Development 2014)
* Koops B. J., 'Commanding decryption and the privilege against self-incrimination', in Breur C. M., Kommer M. M., Nijboer J. F. and Reijntjes J. M. (Eds), *New trends in criminal investigation and evidence, Volume II* (Intersentia 2000)
* Koops B., 'Should ICT regulation be technology-neutral?' in Koops B., Lips M., Prins C. and Schellekens M., *Starting points for ICT regulation. Deconstructing prevalent policy one-liners* (Asser Press 2006)
* Kraut R. E., Lewis S. H. and Swezey L. W., 'Listener responsiveness and the coordination of conversation' (1982) 43 Journal of personality and social psychology 718
* Kushner D., "Anonymous v. Steubenville" (Rolling Stone, 27 November 2013), <http://www.rollingstone.com/culture/news/anonymous-vs-steubenville-20131127>
* Lagodny O., *Expert Opinion for the Council of Europe on Questions Concerning Double Criminality*, PC-OC/WP (2004)
* Landreth B., *Out of the Inner Circle: a Hacker's Guide to Computer Security* (Microsoft Press 1985)
* Lasse Lueth K., 'State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating' (IoT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>
* Lasse Lueth K., 'State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating' (IOT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>
* Lastowka F. G. and Hunter D., 'Virtual crimes', (2004) 49 New York law School Law Review 293
* Laumann E. O., Siegel P. M and Hodge R. W. (Eds), *The logic of social hierarchies* (Markham 1970)

* Lauterwein C. C., *The Limits of Criminal Law: A Comparative Analysis of Approaches to Legal Theorizing* (Ashgate Publishing 2013)
* Leiner B. M. *et al.*, 'A brief history of the Internet' (2009) 39 ACM SIGCOMM Computer Communication Review 22
* Leone L., 'Il nuovo danneggiamento informatico', (2010) 1 Ciberspazio e Diritto 211
* Lepage A., Maistre du Chambon P. and Salomon R., *Droit Penal des Affaires* (LexisNexis 2015)
* Levi M., Smith A., *A comparative analysis of organised crime conspiracy legislation and practice and their relevance to England and Wales* (Home Office Online 2002)
* Levy S., *Hackers: Heroes of the computer revolution* (Penguin Books 2001)
* Li X., 'Hacktivism and the First Amendment: Drawing the Line between Cyber Protests and Crime' (2013) 27 Harvard Journal of Law and Technology 301
* Liberty, 'Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Commons' (March 2016), <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20summary%20of%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>
* Liberty, *Liberty's response to the Home Office consultation on the Equipment Interference Code of Practice* (March 2015), <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20response%20to%20the%20Home%20Office%20consultation%20on%20the%20Equipment%20Interference%20Code%20of%20Practice%20%28Mar%202015%29.pdf>
* Licciardello C., 'Fostering International Cooperation on Cybersecurity: a Global Response to a Global Challenge', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)
* Lin P., 'Why ethics matters for autonomous cars' in Maurer M., Gerdes J. C., Lenz B., Winner H. (Eds) *Autonomous Driving* (Springer 2016)
* Liu S., 'Blockchain technology market size worldwide 2018-2023' (Statista.com. 9 August 2019), <https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/>
* Loeffler R., *Report of the trustee of the Equity Funding Corporation of America* (1974)
* Luban D., O'Sullivan J. R. and Stewart D. P., *International and Transnational Criminal Law* (Aspen 2010)
* Ludlow P., 'New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures', in Ludlow P. (Ed), Crypto Anarchy, Cyberstates, and Pirate Utopias (MIT Press 2001)

* Macdonald S., 'Cyberterrorism and Enemy Criminal Law' in Finkelstein C., David Ohlin J. and Govern K. (Eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015)
* MacEwan N. F., 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 Criminal Law Review 955
* Maniscalco A., 'Public Spaces, Marketplaces, and the Constitution: Shopping Malls and the First Amendment' (SUNY Press, 2015)
* Manuel Gómez Benítez J., 'El dominio del hecho en la autoría (validez y límites)', (1984) 37 Anuario de derecho penal y ciencias penales 103
* Marberth-Kubicki A., *Computer-und Internetstrafrecht* (CH Beck 2010)
* Marshall Jarrett H. and Bailie M. W., 'Prosecuting Computer Crimes' (Office of Legal Education - Executive Office for United States Attorneys 2010)
* Martin R. S., 'Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome', (2003) 40 American Criminal Law Review 1271
* Mason S. (Ed), *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths 2007)
* Masuda Y., *The Information Society: As Post-industrial Society* (World Future Society 1980)
* McCue C., *Data mining and predictive analysis: Intelligence gathering and crime analysis* (Butterworth-Heinemann 2014)
* McGinn R. E., *Science, Technology, and Society* (Prentice Hall1991)
* McLaurin J., 'Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks' (2011) 30 Yale Law & Policy Review 211
* Meet Hackers Editorial Team, "Ghostbin a New Form of Pastebin" (MeetHackers.com, 16 May 2014) <http://www.meethackers.com/2014/05/ghostbin-new-form-of.html>
* Melander S., 'Ultima Ratio in European Criminal Law' (2013) 3 Oñati Socio-Legal Series 1
* Menthe D. C., 'Jurisdiction in Cyberspace: A Theory of International Spaces', (1998) 4 Michigan Telecommunications and Technology Law Review 69
* Mercer D., "Technology and the law: dealing with the 'law lag'" (The Australian, 4 July 2011), <http://www.theaustralian.com.au/archive/business/technology-and-the-law-dealing-with-the-law-lag/news-story/b312d05074f757b67cfbe74d9d85615c>
* Merleau-Ponty M., *Phénoménologie de la perception* (Gallimard, 1945)
* Meyers C., Powers S. and Faissol D., 'Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches' (U.S. Department of Energy
Office of Scientific and Technical Information 2009)
* Miller A. R., *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Mass Market 1971)

* Miller K., 'Total surveillance, big data, and predictive crime technology: privacy's perfect storm', (2014) 19 Journal technology of law and policy 105
* Mitchell M. and Mitchell N., '5 Amazing Ways WARGAMES Changed the World' (TheGeek Twins, 6 April 2014) <http://www.thegeektwins.com/2014/06/5-amazing-ways-wargames-changed-world.html#.Vurr5bReSng>
* Mitsilegas V., *Justice and Trust in the European Legal Order* (Jovene 2016)
* Mnookin J. L., 'Virtual(ly) Law: The Emergence of Law in LambdaMOO', (1996) 2 Journal of Computer Mediated Communication 1
* Moore R., *Cybercrime: Investigating High-Technology Computer Crime* (Rutledge 2010)
* Morgan S., 'Cyber Attacks By Insiders Result In Devastating Costs To Organizations Globally' (Cybercrime Magazine, 11 June 2018) <https://cybersecurityventures.com/cyber-attacks-by-insiders-result-in-devastating-costs-to-organizations-globally/>
* Morozov E., 'In Defence of DDoS' (Slate, 13 December 2010) <http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html>
* Mousnier R., *Social hierarchies, 1450 to the present* (Schocken 1973)
* Mumford L., *Technics and Civilization* (The University of Chicago Press 2010)
* Murphy C. T., 'International Law and the Internet: An Ill-Suited Match', (2002) 25 Hastings International and Comparative Law Review 405
* Murray G., 'United against Cybercrime: the UNODC/ITU Cybercrime Capacity Building Initiative', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)
* Nadelmann E. A., 'Global Prohibition Regimes: The Evolution of Norms in International Society', (1990) 44 International Organisation 479
* Necessary & Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), <https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf>
* O'Connel J., 'Stanford Scholar: Us Unlikely to Prosecute Anonymous for Harassing Isis' (Hacked, 24 November 2015) <https://hacked.com/stanford-scholar-us-unlikely-prosecute-anonymous-harassing-isis/>
* OECD, *Computer-related criminality: Analysis of Legal Politics in the OECD Area* (ICCP series n. 10, 1986)
* Oerlemans J. J., 'Hacking without a legal basis' (Leiden Law Blog, 30 October 2014) <http://leidenlawblog.nl/articles/hacking-without-a-legal-basis>.

* Ohlin J. D., 'Co-Perpetration German Dogmatik or German Invasion?', in Stahn C. (Ed), *The Law and Practice of the International Criminal Court: A Critical Account of Challenges and Achievements* (OUP 2015)
* Ohlin J. D., 'Group Think: The Law of Conspiracy and Collective Reason', (2007) 98 Journal of Criminal Law and Criminology 147
* Oikarinen J. and Reed D., *Request for Comments n. 1459. Internet Relay Chat Protocol* (May 1993)
* Okoth J., *The Crime of Conspiracy in International Criminal Law* (Springer 2014)
* Oliva L., 'Is DDoS the New 'Sit-In'?' (Vice, 25 January 2013) <http://motherboard.vice.com/blog/is-ddos-the-new-civil-disobedience>
* Olson P., *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Little Brown & Company 2013)
* Orlandi R., 'Questioni attuali in tema di processo penale e informatica', (2009) 1 Rivista di Diritto Processuale 129
* Ormerod D., *Smith and Hogan Criminal Law: Cases and Materials* (OUP 2005)
* Osula A., 'Transborder access and territorial sovereignty', (2015) 31 *Computer Law & Security Review* 719
* Paganini P., 'Hacking Drones: Overview of the Main Threats' (Infosec, 4 June 2013) <http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats>
* Papa M., *Fantastic voyage: Attraverso la specialità del diritto penale* (Giappichelli 2019)
* Pardo F., *Le groupe en droit penal* (PAR, 2009)
* Parker D. B., *Crime by Computer* (Scribner 1976)
* Patrone I., 'Conflicts of jurisdiction and judicial cooperation instruments: Eurojust's role', (2013) 2 Era Forum 215
* Paulucci C. M., *Cooperazione giudiziaria e di polizia in material penale* (UTET 2011)
* Paulussen C., *Male captus bene detentus? Surrendering Suspects to the International Criminal Court* (Intersentia, 2010)
* Paust J. *et al* (Eds), *International Criminal Law: Cases and Materials* (Carolina Academic Press 1996)
* Peers S., Hervey T., Kenner J. and Ward A., *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014)
* Pellissero M., *Reati contro la personalità dello stato e contro l'ordine pubblico* (Giappichelli 2010)
* Peristeridou C., 'The Principle of Legality', in J. Keiler and D. Roef (Eds), *Comparative Concepts of Criminal Law* (Intersentia 2016)
* Pfleeger S. L., Predd J. B., Hunker J., Bulford C., 'Insiders behaving badly: Addressing bad actors and their actions', (2010) 5 IEEE Transactions on Information Forensics and Security 169

* Picotti L. and Salvadori I., *National legislation implementing the Convention on Cybercrime: comparative analysis and good practices,* CoE Project on Cybercrime, Discussion Paper (2008)
* Picotti L., 'Expanding Forms of Preparation and Participation - General Report', (2007) 3 Revue Internationale de Droit Pénal 405
* Picotti L., 'I profili penali delle comunicazioni illecite via Internet', (1999) Diritto dell'Informazione e dell'Informatica 288
* Picotti L., 'Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale' (2005) 2 Diritto dell'Internet 189
* Pollicino O. and Romeo G. (Eds), *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe* (Routledge 2016)
* Portesi S., 'Attacks against information systems: an analysis of aspects related to illegal access', (2004) 5 Ciberspazio e diritto 411
* Portnoy M. and Goodman S. (Eds), *Global Initiatives to Secure Cyberspace* (Springer 2009)
* Postmes T., Spears R., Sakhel K. and De Groot D., 'Social influence in computer-mediated communication: The effects of anonymity on group behavior' (2001) 27 Personality and Social Psychology Bulletin 1243
* Prince M., 'The DDoS That Almost Broke the Internet' (Cloudflare 27 March 2013) <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/>
* Privacy International, *Hacking Safeguards and Legal Commentary* (privacyinternational.org, 11 June 2018), <https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary>
* Protalinski E., 'Pastebin to hunt for hacker pastes, Anonymous cries censorship' (Zero Days, 4 April 2012) <http://www.zdnet.com/article/pastebin-to-hunt-for-hacker-pastes-anonymous-cries-censorship/>
* Quick D., Choo K. R., 'Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive' (2014) 480 Trends & Issues in Crime and Criminal Justice 1
* Quirico S., 'Il modello organizzativo delle Brigate Rosse in una prospettiva comparata' (2008) 44 Quaderni di storia contemporanea 1
* Radware Security, *DDoS Survival Handbook* (2015)
* Ram C., 'Cybercrime', in Boister N. and Currie R. J. (Eds), *Routledge Handbook of Transnational Criminal Law* (Routledge 2014)
* Ramage S., *Privacy-Law of Civil Liberties* (iUniverse, 2007)

* Re R. M. and Solow-Niederman A., 'Developing Artificially Intelligent Justice' (2019) 22 Stanford Technology Law Review 242
* Reinsel D., Gantz J. and Rydning J. (Eds), *The Digitization of the World From Edge to Core* (IDC White Paper 2018)
* Resta S., 'Informatica, telematica e computer crimes' (1997) 6 Informatica e diritto 143
* Rhodes R., *Organized Crime: Crime Control vs. Civil Liberties* (Random House 1984)
* Ribero J., 'After Lavabit, Silent Circle also shuts down its encrypted email service' (PCWorld, 9 August 2013) <https://www.pcworld.com/article/2046264/after-lavabit-silent-circle-also-shuts-down-email-service.html>
* Richmond S. and Williams C., 'Millions of internet users hit by massive Sony PlayStation data theft' (The Telegraph, 26 April 2011), <http://www.telegraph.co.uk/technology/sony/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html>
* Richter F., 'WhatsApp Usage Shows No Signs of Slowing Down' (Statista.com, 7 May 2018) <https://www.statista.com/chart/13762/whatsapp-messages-sent-per-day/>
* Ricker Schulte S., *Cached: Decoding the Internet in Global Popular Culture* (NYU Press 2013)
* Ritleng D., 'The Contribution of the Court of Justice to the Structuring of the European Space of Fundamental Rights', (2014) 5 New Journal of European Criminal Law 507
* Rogers M. K., 'A two-dimensional circumplex approach to the development of a hacker taxonomy' (2006) 3 Digital Investigation 97
* Ronfeldt D., *Tribes, Institutions, Markets, Networks: A Framework About Societal Evolution* (RAND Corporation 1996)
* Rossi F., 'The European harmonisation of the general part of criminal law' (2017) 5 Rivista Italiana di Diritto Pubblico Comunitario 1077
* Ruggeri S. (Ed), *Human Rights in European Criminal Law: New Developments in European Legislation and Case Law after the Lisbon Treaty* (Springer 2015)
* Saleh I., Ammi M. and Szoniecky S. (Eds) *Challenges of the Internet of Things: Technique, Use, Ethics* (John Wiley & Sons 2018)
* Salvador J. W., 'Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime' (2015) 41 Rutgers Computer & Technology Law Journal 268
* Salvadori I., 'L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica', in Picotti L. (Ed), *Tutela penale della persona e nuove tecnologie* (CEDAM 2013)
* Sànchez-Cuenca I., 'The Dynamics Of Nationalist Terrorism: ETA and the IRA' (2007) 19 Terrorism and Political Violence 289

* Sanders G., 'The Very Real Dangers of Hacked Drones' (Tractica, 4 September 2019) <https://www.tractica.com/robotics/the-very-real-dangers-of-hacked-drones/>
* Sangero B., 'Are All Forms of Joint Crime Really 'Organized Crime'? On the New Israeli Combating Criminal Organizations Law and Parallel Legislation in the US and Other Countries," (2007) 29 Loyola of Los Angeles International and Comparative Law Review 61
* Saul B., Defining Terrorism in International Law, 180 (OUP 2008)
* Sauter M., *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet* (Bloomsbury, 2014)
* Schjolberg S. and Ghernaouti-Helie S., *A Global Treaty on Cybersecurity and Cybercrime* (AitoOslo 2011)
* Schjolberg S., 'Potential New Global Legal Mechanisms on Combating Cybercrime and Global Cyberattacks', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)
* Schjolberg S., *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva* (2008) <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>
* Schmitt M. N. (Ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)
* Schultheis N., 'Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry' (2014) 9 Brooklyn Journal of Corporate, Financial & Commercial Law 661
* Schultz T., 'Carving up the internet: jurisdiction, legal orders, and the private/public international law interface', (2008) 4 European Journal of International Law 799
* Schwartz M. J., 'Cybercrime Milestone: Guilty Verdict in RICO Case', (Informationweek, 12 December 2013) <http://www.darkreading.com/attacks- and-breaches/cybercrime-milestone-guilty-verdict-in-rico-case/d/d-id/l 113050>
* Scola N., 'Ten Ways to Think About DDoS Attacks and "Legitimate Civil Disobedience"' (Techpresident, 13 December 2010) <http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacks-and-legitimate-civil-disobedience>
* Seger A., 'The Budapest Convention 10 Years in: Lessons Learnt', in Manacorda S. (Ed), *Cibercriminality: Finding a Balance Between Freedom and Security* (ISPAC 2012)
* Seitz N., 'Transborder Search:
A New Perspective in Law Enforcement?', (2005) 7 Yale Journal of Law & Technology 23
* Shabas W., *The European Convention on Human Rights* (OUP 2015)

* Shaefter J., 'Sex and the simulated city: virtual world raises issues in the real one' (Michigan News, 27 January 2004) <http://web.archive.org/web/20050716075604/http://www.freep.com/news/mich/sims27_20040127.htm>
* Shammas J., 'Anonymous hacker reveals how they will destroy ISIS and its ability to carry out terror attacks' (The Mirror, 1 December 2015) <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-693133.1>
* Shaw M. N., *International Law* (OUP 2008)
* Shearer E., 'Social media outpaces print newspapers in the U.S. as a news source' (Pew Research Center, 18 December 2018) <https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/>
* Shumaker R. W., Walkup K. R. and Beck B. B., *Animal Tool Behavior: The Use and Manufacture of Tools by Animals* (The Johns Hopkins University Press 2011)
* Sieber U., 'Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law', in Delmas-Marty M., Pieth M. and Sieber U. (Eds), *Les Chemins de l'Harmonisation Pénale/Harmonising Criminal Law* (Société de législation comparée 2008)
* Sieber U., 'The Forces Behind the Harmonization of Criminal Law', in Delmas-Marty M. (Ed), *Les chemins de l'harmonisation pénale, Harmonising criminal law* (Société de Législation Comparée, 2008)
* Sieber U., *Computercriminalitat und Strafrecht* (Carl Heymanns Verlag KG 1977)
* Sieber U., *Legal Aspects of Computer-related Crime in the Information Society* (Comcrime Study 1998)
* Simma B. and Muller A. T., 'Exercise and limits of jurisdiction,' in J. Crawford *et al* (eds), *The Cambridge Companion to International Law* (CUP 2012)
* Simonato M., 'Defence rights and the use of information technology in criminal procedure', (2014) 85 Revue Internationale de Droit Pénal 261
* Skoudis E., *Malware: Fighting Malicious Code* (Prentice Hall 2004)
* Slivka R. T. and Darrow J. W., 'Methods and Problems in Computer Security' (1976) 5 Rutgers Journal of Computers and the Law 217
* Slobbe J. and Verberkt S. L. C., "Hacktivists: Cyberterrorists or Online Activists?" (2012) arXiv preprint arXiv:1208.4568
* Smith B., 'The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack' (Microsoft, 14 May 2017) <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#lEGOIgXOx20j4QgA.99>

* Smith R. G., 'Transnational Cybercrime and Fraud', in Reichel P. and Albanese J. (Eds), *Handbook of transnational crime and justice* (Sage 2013)
* Smith R. G., Grabosky P. and Urbas G., *Cyber Criminals on Trial* (CUP 2004)
* Smith R., Grabosky P. and Urbas G., *Cyber criminals on trial* (CUP 2004)
* Soble R. L. and Dallos R. E., *The Impossible Dream: The Equity Funding Story* (G.P. Putnam's Sons 1975)
* Sofaer A, D., Grove G. D. and Wilson G. D., 'Draft International Convention To Enhance Protection from Cyber Crime and Terrorism', in Sofaer A. D. and Goodman S. E. (Eds), *The Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution 2001)
* Sofaer A. D., 'Toward an International Convention on Cyber', in A Sofaer A. D. and Goodman S. E. (Eds), *The Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution 2001)
* Solarz A., *Computer Technology and Computer Crime* (National Swedish Council for Crime Prevention, Research and Development Division 1981)
* Song H., Rawat D. B., Jeschke S., Brecher C. and Kaufmann M. (Eds) *Cyber-Physical Systems: Foundations, Principles and Applications* (Elsevier 2016)
* Spain, Cuerpo Nacional de Policia, Nota de Prensa, 'La Policía Nacional desarticula la cúpula de la organización "hacktivista" Anonymous en España' (10 June 2011) <http://www.policia.es/prensa/20110610_2.html>
* Stalbaum B., 'The Zapatista Tactical FloodNet: A collabortive, activist and conceptual art work of the net' (Tactical Media File, 07 August 2010) <http://www.tacticalmediafiles.net/articles/3394/The-Zapatista-Tactical-FloodNet>
* Stay R. J., 'Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann', (1996) 13 Georgia State University Law Review 581
* Stephenson N., *Snow Crash* (Bantam Books 1992)
* Sterling B., *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (Bantam Books 1992)
* Stewart J., 'The End of Modes of Liability for International Crimes', (2012) 25 Leiden Journal of International Law 165
* Stoll C., *The Cuckoo's Egg* (Doubleday 1989)
* Strate L., 'The varieties of cyberspace: Problems in definition and delimitation' (1999) 63 Western Journal of Communication 382
* Strati S., "Il Codice della 'Ndrangheta'" (1992) 26 Forum Italicum: A Journal of Italian Studies 281
* Suárez López J. M., 'Aspectos dogmáticos y político criminales en el tratamiento penal de la delincuencia organizada', (2012) 30 Anales De Derecho 90

* Suler J., 'The online disinhibition effect' (2004) 7 Cyberpsychology & Behavior 321
* Sullivan B., 'FBI Software Cracks Encryption Wall', (NBS News, 20 November 2001) <http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.WdOKTUyB1mA>
* Summers S., Schwarzenegger C., Ege G. and Young F., *The Emergence of EU Criminal Law* (Hart Publishing, 2014)
* SurfWatch Labs, 'Anonymous Ops Trending, Where are The Other Hacktivists?' (SurfWatch, 26 May 2016) <https://blog.surfwatchlabs.com/2016/05/26/anonymous-ops-trending-government-targeted-where-are-the-other-hacktivists/>
* Symantec, *Executive Report: Smart Cities. Transformational 'Smart Cities': Cyber Security And Resilience* (2013)
* Szmigiera M., 'Number of Blockchain wallet users globally 2016-2019' (Statista.com, 7 October 2019), <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/>
* Taber J. K., 'A survey of computer crime studies.' (1980) 2 Computer Law Journal 275
* Thaman S. C. (Ed), *Exclusionary Rules in Comparative Law* (Springer Science & Business Media 2012)
* Thomson J. J., "The right to privacy", (1975) Philosophy and public affairs 295
* Tikk E. and Kaska K., 'Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons', in J. Demergis (Ed), *ECIW2010 - 9th European Conference on Information Warfare and Security* (Academic Publishing Limited 2010)
* Toomey F., 'Data, The Speed Of Light And You' (Techcrunch, 8 November 2015) <https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/>
* Traynor I., 'Russia accused of unleashing cyberwar to disable Estonia' (The Guardian, 17 May 2007) <http://www.theguardian.com/world/2007/may/17/topstories3.russia>
* Turner R. H. and Killian L. M., *Collective Behavior* (Prentice Hall 1959)
* UE, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement* (2017)
* UK, Government, *Serious Crime Act 2015 Fact sheet: Part 2: Computer* misuse <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf>
* UK, Home Office, *Factsheet – Investigatory Powers Commission", Investigatory Power Bill* (2015), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473744/Factsheet-Investigatory_Powers_Commission.pdf>

* UK, Home Office, *Factsheet – Oversight: Investigatory Power Bill* (2015), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473741/Factsheet-Oversight.pdf>
* UK, *Investigatory Powers Bill: Equipment Interference,* <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530554/Equipment_Interference_Factsheet.pdf>
* UNODC, *Comprehensive Study on Cybercrime* (UN 2013)
* US, Department of Defence, *US Strategy for Homeland Defense and Civil Support* (2005)
* US, Department of Justice, Office of Public Affairs, Press Release, 'Member of Organization That Operated Online Marketplace for Stolen Personal Information Sentenced to 20 Years in Prison' (15 May 2014) <https://www.justice.gov/opa/pr/member-organization-operated-online-marketplace-stolen-personal-information-sentenced-20>
* US, Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002)
* US, District of Nevada, Attorney's Office, Press Release, 'Man Who Bought and Sold Stolen Personal Information Online Convicted of Participating in Racketeering Organization' (6 December 2013) <https://www.justice.gov/usao-nv/pr/man-who-bought-and-sold-stolen-personal-information-online-convicted-participating>
* US, Federal Bureau of Investigation, *Organized Crime* <https://www.fbi.gov/investigate/organized-crime>
* Usborne D., 'Bowman Avenue Dam: US in fear of new cyber attack as dam breach by Iranian hackers is revealed' (The Independent 21 December 2015) <http://www.independent.co.uk/news/world/americas/bowman-avenue-dam-us-in-fear-of-new-cyber-attack-as-dam-breach-by-iranian-hackers-is-revealed-a6782081.html>
* Vaciago G., 'Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics', in *CYBERLAWS 2012, The Third International Conference on Technical and Legal Aspects of the e-Society* (Berntzen 2012)
* Vaciago G., 'Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato' (Giappichelli 2012)
* Van De Velde P., 'EU Council takes action against attacks on information systems', (2005) Bird & Bird
* Van Den Wyngaert C. and Stessens G., 'The international non bis in idem principle: resolving some of the unanswered questions', (1999) 4 International and Comparative Law Quarterly 779
* Van der Vleuten E. and Lagendijk V., 'Transnational infrastructure vulnerability: The historical

shaping of the 2006 European "Blackout"' (2010) 38 Energy Policy 2042

* van der Wilt H., 'On the Hierarchy between Extradition and Human Rights', in De Wet E. and Vidmar J. (Eds), *Hierarchy in International Law: The Place of Human Rights* (OUP 2012)
* Van Lawick-Goodall J., 'Tool-using in primates and other vertebrates' in Lehrman D. S., Hinde R., Shaw E. (Eds) *Advances in the Study of Behavior, Vol. 3* (Academic Press 1970)
* van Sliedregt E., *Individual Criminal Responsibility in International Law* (OUP 2012)
* Vedaschi A. and Lubello V., 'Data retention and its implications for the fundamental right to privacy: A European perspective' (2015) 20 Tilburg Law Review 14
* Vitkauskas D. and Dikov G., 'Protecting the right to a fair trial under the European Convention on Human Rights', *Council of Europe human rights handbooks* (2012)
* Volz D. and Raymond N., 'U.S. to blame Iran for cyber attack on small NY dam' (Reuters 10 March 2016) <http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WC2NH>
* Walden I., 'Addressing the Data Problem: The Legal Framework Governing Forensics in an Online Environment', in Jensen C., Poslad S., Dimitrakos T. (Eds), *Trust Management* (iTrust 2004)
* Warren S. and Brandeis L., 'The Right to Privacy' (1890) 4 Harvard Law Review 193
* Wasik M., 'The Computer Misuse Act 1990', (1990) Criminal Law Review 767
* Watney M., 'Cybercrime Regulation at a Cross-Road: State and Transnational Laws Versus Global Laws', in *International Conference on Information Society* (IEEE 2012)
* Webster F., *Theories of Information Society* (Routledge 2007)
* Wechsler H., 'Codification of Criminal Law in the United States: The Model Penal Code' (1968) 8 Columbia Law Review 1425
* Whatsapp, "Security" <https://www.whatsapp.com/security/>
* White R. C.A. and Ovey C., *The European convention on human rights* (OUP 2010)
* Williams S., 'Human Rights Safeguards and International Cooperation in Extradition: Striking the Balance', (1992) 3 Criminal Law Forum 191
* Witt P. L., 'Internet Relay Chat', in Bidgoli H. (Ed), *Handbook of Information Security, Key Concepts, Infrastructure, Standards, and Protocols* (John Wiley and Sons 2006)
* Wolfendale J., 'My avatar, my self: Virtual harm and attachment', (2007) 9 Ethics and Information Technology 111
* Woo C. and So M., 'The case for Magic Lantern: September 11 Highlights. A need for increased surveillance', (2002) 15 Harvard Journal of Law & Technology 521
* World Information Technology and Services Alliance, *Statement on the Council of Europe Draft Convention on Cyber-Crime* (2000) <www.witsa.org/papers/COEstmt.pdf>

* Yadron D., Ackerman S. and Thielman S., 'Inside the FBI's encryption battle with Apple' (The Guardian, 18 February 2016) <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>
* Zacchè F., "L'acquisizione della posta elettronica nel processo penale", (2013) 4 Processo Penale e Giustizia 103
* Zambo S., 'Digital La Cosa Nostra: The Computer Fraud and Abuse Act's failure to punish and deter organized crime', (2007) 33 New England Journal on Criminal and Civil Confinement 551
* Ziccardi G., 'Cybercrime and Jurisdiction in Italy', in Brenner S. W. and Koops B. J. (Eds), *Cybercrime and Jurisdiction: A Global Survey* (Springer 2006)
* Zimmermann R., *La coopération judiciaire internationale en matière pénale* (Stämpfli 2009)
* Zimring F. E. and Johnson D. T., 'Public opinion and the governance of punishment in democratic political systems', in *The Annals of the American Academy of Political and Social Science* (2006)
* —'#AnonOps Channel Rules' < http://anonops.com/chanrules.html>
* —'Anon Ops, A Press Release' (10 December 2010) <http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf>
* —'Anon-combat-index: What is Anonymous?' <https://ghostbin.com/paste/tfgst>
* —'Anonymous Presents: The Onion IRC' <http://www.anonymousvideo.eu/anonymous-presents-the-onion-irc.html>
* —'Capitain Zap' (Hack Story, 2011) <http://hackstory.net/Captain_Zap>
* —'Chaos Computer Club analyzes government malware' (CCC, 8 October 2011) <https://ccc.de/en/updates/2011/staatstrojaner>
* —'Connecting One Billion Users Every Day' (WhatsApp Blog, 26 July 2017), <https://blog.whatsapp.com/10000631/Connecting-One-Billion-Users-Every-Day>
* —'Cyber Attacks on the Ukrainian Grid:
What You Should Know' (FireEye, 2016) <https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf>
* —'DDoS Attacks 101: Types, targets, and motivations' (Calyptix, 26 April 2015) <http://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/>
* —'DDoS attacks continue to rise in size, frequency and complexity. Are you prepared to stop them before they impact the availability of your business?' (Arbor Networks) <https://www.arbornetworks.com/ddos-protection-products>

* —‘DDOS Trends to Watch for in 2020’ (EC-Council, 19 December 2019) < https://blog.eccouncil.org/ddos-trends-to-watch-for-in-2020/>
* —‘Facebook Operational Guidelines for Law Enforcement Authorities’ <https://www.facebook.com/safety/groups/law/guidelines/>
* —‘How Many Products Does Amazon Sell?’ (Scapehero, April 2019) <https://www.scrapehero.com/number-of-products-on-amazon-april-2019/>
* —‘How to kill drones’ <http://anoncentral.tumblr.com/post/42515581659/how-to-kill-drones>
* —‘Industry group still concerned about draft Cybercrime Convention’ (Out-Law 5 December 2000) <www.out-law.com/page-1217>
* —‘ITU releases 2018 global and regional ICT estimates: For the first time, more than half of the world's population is using the Internetp (ITU, 7 December 2018) <https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx>
* —‘John Suler's The Psychology of Cyberspace’ <http://users.rider.edu/~suler/psycyber/disinhibit.html>
* —‘LoveBug – the worm that changed the IT security landscape – is ten years old today’ (Infosecurity Magazine, 4 May 2010) <http://www.infosecurity-magazine.com/view/9184/lovebug/>
* —‘Maps of Internet Service Provider (ISP)
and Internet Backbone Networks’, <http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/isp_maps.html>
* —‘Number of smartphone users worldwide from 2016 to 2021 (in billions)’ (Statista, 26 June 2019) <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>
* —‘Philippines’ Laws Complicate Virus Case’ (USA Today, 7 June 2000)
* —‘Postulates: An Anonymous Manifesto’ <http://anonnews.org/press/item/199>
* —‘Q&A: UK filters on legal pornography’ (BBC, 22 July 2012) <http://www.bbc.co.uk/news/technology-23403068>
* —‘Ukraine power cut 'was cyber-attack'’ (BBC, 11 January 2017) <http://www.bbc.com/news/technology-38573074>
* —(Note), ‘Limitations on the Federal Judicial Power to Compel Acts Violating Foreign Law’, (1963) 63 Columbia Law Review 1441
* —(Note), ‘The Conspiracy Dilemma: Prosecution of Group Crime or Protection of Individual Defendants’, (1948) 62 Harvard Law Review 276

CASE LAW

* Belgium, Hof van Cassatie - Cour de Cassation, *20 February 1991*
* Belgium, Hof van Cassatie - Cour de Cassation, *1 December 2015*
* CJEU, *Åklagaren v Åkerberg Fransson* Case 617/10 (2013)
* CJEU, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined cases C-293/12 and C-594/12, 8 April 2014
* CJEU, *Commission v Greece (Greek Maize)*, Case 68/88, 21 September 1989
* CJEU, *Criminal proceedings against Silvio Berlusconi* (Case 387/02*), Sergio Adelchi* (Case 391/02*) and Marcello Dell'Utri and Others* (Case 403/02), Opinion of Advocate General Kokott, 14 October 2004
* DK, Eastern High Court, *U 1987.216*
* ECJ, *Commission v. Council*, Case 440/05 ("ship-source pollution case"), 23 October 2007
* ECtHR, *Al-Skeini and Others v. the United Kingdom* (Application n. 55721/07), 7 July 2011
* ECtHR, *Aldemir v Turkey* (Application n. 32124/02), 18 December 2007
* ECtHR, *Allen v. the United Kingdom* (Application n. 25424/09), 12 July 2013
* ECtHR, *Andersson v. Sweden* (Application n. 20022/92), 25 February 1992
* ECtHR, *Appleby and Others v. The United Kingdom*, (Application n. 44306/98), 6 May 2003
* ECtHR, *Ashughyan v. Armenia* (Application n. 33268/03), 17 July 2008
* ECtHR, *Association Confraternelle de la Judiciaire v. France* (Application n. 49526/15), pending
* ECtHR, *Balçık and Others v. Turkey* (Application n. 25/02), 29 November 2007
* ECtHR, *Big Brother Watch and Others v. The United Kingdom* (Applications n. 58170/13, 62322/14 and 24960/15), 13 September 2018
* ECtHR, *Cantoni v. France* (Application n. 17862/91), 15 November 1996
* ECtHR, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Applications n, 293/12 and n. 594/12), 8 April 2014
* ECtHR, *Gäfgen v. Germany* (Application n. 22978/05), 1 June 2010
* ECtHR, *Issa and Others v. Turkey* (Application n. 31821/96), 16 November of 2004
* ECtHR, *Jalloh v. Germany* (Application n. 54810/00), 11 July 2006
* ECtHR, *Khan v. the United Kingdom* (Application n. 35394/97), 12 May 2000
* ECtHR, *Klass and others v. Germany*, (Application n. 5029/71), 6 September 1978.
* ECtHR, *Kokkinakis v Greece* (Application n. 14307/88), 25 May 1993
* ECtHR, *Kruslin v. France* (Application n. 11801/85), 24 April 1990

* ECtHR, *Leander v Sweden* (Application n. 9248/81) 26 March 1987
* ECtHR, *Letellier v. France* (Application n. 12369/86), 26 June 1991
* ECtHR, *Malone v. the United Kingdom* (Application n. 8691/79), 2 August 1984
* ECtHR, *O'Halloran and Francis v. United Kingdom* (Application n. 15809/02 and 25624/02), 29 June 2007
* ECtHR, *Olsson v. Sweden* (Application n. 10465/83), 24 March 1988
* ECtHR, *Oya Ataman v. Turkey* (Application n. 74552/01), 5 December 2006
* ECtHR, *PG and JH v. UK* (Application n. 44787/98), 25 September 2001
* ECtHR, *Prado Bugallo v. Spain* (Application N. 58496/00), 18 February 2003
* ECtHR, *Privacy International and Others v. The United Kingdom* (Application n. 46259/16), pending
* ECtHR, *Rassemblement Jurassien and Unité Jurassienne v Switzerland* (Application n. 8191/78), 10 October 1979
* ECtHR, *Roman Zakharov v. Russia* (Application n. 47143/06), 4 December 2015
* ECtHR, *Saunders v. United Kingdom* (Application n. 19187/91), 17 December 1996
* ECtHR, *Sergey Zolotukhin v. Russia* (Application n. 14939/03), 10 February 2009
* ECtHR, *Soering v. the United Kingdom* ((Application n. 14038/88), 7 July 1989
* ECtHR, *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria* (Application n. 29221/95 and 29225/95), 2 October 2001.
* ECtHR, *Szabó and Vissy v. Hungary* (Application n. 37138/14), 12 January 2016
* ECtHR, *Vasileva v. Denmark* (Application n. 52792/99), 25 September 2003
* ECtHR, *Weber & Saravia v. Germany* (Application n. 54934/00), 29 June 2006
* FR, Cour d'Appel de Aix-en-Provence, *2 juin 1993*
* FR, Cour d'Appel de Paris, *15 decembre 1999*
* FR, Cour de Cassation, *8 juillet 2015, n° de pourvoi 14-88329*
* FR, Cour de Cassation, *in re Urios 1919-1922, Ann. Dig. 107, No. 70*
* FR, Tribunal de Grande Instance de Nancy, *26JIRS/2015, 14357000066, 23 November 2015*
* GER, Bundesgerichtshof, *Urt. v. 12. 12. 2000 – 1 StR 184/00*
* GER, Bundesverfassungsgericht, *Urt. v 15. 12. 1983 - 1 BvR 209/83*
* GER, OLG Frankfurt 1, *Strafsenat 1 Ss 319/05, 22.05.2006*.
* International Court of Justice, *Democratic Republic of the Congo v. Belgium*, I.C.J. Reports 2002, 77, 14 February 2002
* International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004

* International Criminal Court, *Situation in the Democratic Republic of the Congo, Lubanga Case*, Decision on Confirmation of Charges, ICC-01/04-01/06-803, PTC I, 29 January 2007
* ITA, Cassazione Penale, *Judgement n. 31389/08*
* ITA, Cassazione Penale, *Judgement n. 50620/13*
* ITA, Cassazione Penale, *Judgement n. 50620/13*
* ITA, Cassazione Penale, *Judgement n. 50620/13*
* ITA, Cassazione Penale, *Judgement n. 8296/04*
* ITA, Cassazione Penale, *Judgement n. 20451/13*
* ITA, Cassazione Penale, *Judgement n. 3886/12*
* ITA, Cassazione Penale, *Judgement n. 43656/10*
* ITA, Cassazione Penale, *Judgement n. 21606/09*
* ITA, Cassazione Penale, *Judgement n. 42635/04*
* ITA, Cassazione Penale, *Judgement n. 3340/99*
* ITA, Cassazione Penale, *Judgement n. 1282/96*
* ITA, Cassazione Penale, *Judgement n. 46156/13*
* ITA, Cassazione Penale, *Judgement n. 50620/13*.
* ITA, Cassazione Penale, *Judgement n. 16307/11*
* ITA, Cassazione Penale, *Judgement n. 16556/09*
* ITA, Cassazione Penale, *Judgement n. 44830/04*
* ITA, Cassazione Penale, *Judgement n. 12732/00*
* ITA, Cassazione Penale, *Judgment n 24695/09*
* ITA, Cassazione Penale, *Judgment n. 254865/12*
* ITA, Cassazione Penale, *Judgment n. 3065/99*
* ITA, Cassazione Penale, *Judgment n. 3067/99*
* ITA, Corte Costituzionale, *Judgement n. 263/10*
* ITA, Tribunale di Catania, Ufficio del Giudice per le Indagini Preliminari, *Decreto di archiviazione, 15 luglio 2019*
* Permanent Court of International Justice, *S.S. Lotus (France v. Turkey)*, SER. A n. 10, 7.9.1927
* Spain, Juzgado de lo Penal, Gijón, *Procedimiento Abreviado No 385/15,* 6 July 2016
* Spain, Tribunal Supremo, *STS 20/01/2009, STS 25/11/2008*
* Special Tribunal for Lebanon, Appeal Chamber, *Interlocutory Decision on the Applicable law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, Case No. STL-ll-0111, 16 February 2011
* The Netherlands, Hoge Raad der Nederlanden, *HR 31 January 2012*

* UK, *R v Christopher Weatherhead, Ashley Rhodes, Peter Gibson, and Jake Burchall*, unreported, Southwark Crown Court, 24 January 2013
* UK, *Cox v Riley*, [1986] 83 Cr App R 54, DC
* UK, *DPP v Lennon* [2006] EWCH 1201
* UK, *Joyce v. Director of Public Prosecution* [1946] AC 347
* UK, *R v Gold and Schifreen* [1988] AC 1063, HL; [1987] 1 QB 1116, CA
* UK, *R v Whiteley*, [1991] 93 Cr App R 25, CA
* UK, *R v. Lennon*, Judgment of District Judge Kenneth Grant, sitting as a Youth Court in Wimbledon, 2 November 2005
* UK, *Re Wood Pulp* [1998] 4 C.M.L.R 901
* UN, Committee Against Torture, *Chipana v. Venezuela*, CAT/C/21/D/110/1998, 10 November 1998,
* UN, Human Rights Committee, *A.P. v. Italy*, Communication No.204/1986, CCPR/C/31/D/204/1986, 16 July 1986
* UN, Human Rights Committee, *Chitat Ng v. Canada*, Communication No. 469/1991, U.N. Doc. CCPR/C/49/D/469/1991, 7 January 1994
* UN, Human Rights Council, *Lopez Burgos v Uruguay*, *Saldias de Lopez (on behalf of Lopez Burgos) v Uruguay*, Merits, Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979, IHRL 2796 (UNHRC 1981), 29 July 1981
* US, *Bragg v. Linden Research*, Inc., 487 F.Supp.2d 593 (E.D.Pa., 2007)
* US, *Grayned v. City of Rockford* - 408 U.S. 104 (1972)
* US, *Harrison v. United States*, 7 F2d 259 (2d cir 1925)
* US, *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y., 2014)
* US, *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945);
* US, *Knight First Amendment Inst. at Columbia Univ. v. Trump*, No. 1:17-cv-5205 (S.D.N.Y.), No. 18-1691 (2d Cir.)
* US, *Krulewitch v. United States*, 336 US 440 (1949)
* US, *Lauritzen v. Larsen*, 345 U.S. 571 (1953)
* US, *Milliken v. Meyer*, 311 U.S. 457 (1940)
* US, *Pulte Homes, Inc. v Laborers' Intern Union of North America*, 648 F 3d 295 (6th Cir. 2011)
* US, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)
* US, *Shad Alliance v. Smith Haven Mall*, 66 NY2d 496, 502 (1985)
* US, *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002)

* US, *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007)
* US, *United States v. Collins*, *et al.*, 13 CR 383 (2013)
* US, *United States v. Conti, 804 F.3d 977, 979-80* (9th Cir. 2015)
* US, *United States v. Cooper, et al.*, 11 CR 471 (2013)
* US, *United States v. David Ray Camez*, No. 2:12-cr-00004-APG-GWF (2014)
* US, *United States v. Lostutter*, 5:16-cr-00062 (2016)
* US, *United States v. Middleton*, 231 F 3d 1207 (9th Cir 2000)
* US, *United States v. Ngige*, 780 F.3d 497, 503 (1st Cir. 2015)
* US, *United States v. Salahuddin*, 765 F.3d 329, 338 (3d Cir. 2014)
* US, *United States v. Ben Laden* (92 F. Supp. 2d 189 (S.D.N.Y. 2000)
* US, *United States v. Blackmer*, 284 U.S. 421, 437 (1932)
* US, *United States v. Dennis Collins, et.al.*, 1:13-cr-383 (2013)
* US, *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996)
* US, *United States v. Jimenez Recio*, 537 US 270, 274 (2003)
* US, *United States v. Liu*, 239 F.3d 138 (2d Cir. 2000)
* US, *United States v. Mitra* 405 F.3d492 (7th Cir.2005)
* US, *United States v. Pascacio-Rodriguez*, 749 F.3d 353, 361-362 (5th Cir. 2014)
* US, *United States v. Rehak*, 589 F.3d 965, 971 (8th Cir. 2009)
* US, *United States v. Werdene*, No. 16-3588 (3d Cir. 2018)
* US, *United States v. Young*, 877 F.2d 1099, 1105-06 (1st Cir. 1989)
* US, *United States v. Yunis*, 681 F.Supp. 896, 1091 (D.D.C. 1988)

LEGISLATION / OFFICIAL DOCUMENTATION

* African Union, (Draft) Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012).
* African Union, *Convention on Cyber Security and Personal Data Protection* (2014)
* Armenia, *Criminal Code*
* Australia, *1979 Australian Telecommunications Interception Act*.
* Austria, *Strafgesetzbuch*
* Belgium, *Code d'Instruction Criminelle / Wetboek van Strafvordering*
* Belgium, *Code Pénal / Wetboek van Strafrecht*
* Belgium, *Loi du 28 novembre 2000 relative à la criminalité informatique*
* Canada, *Criminal Code*
* CoE, *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, ETS 189, 28 January 2003
* CoE, *Convention on Cybercrime,* ETS 185, 23 November 2001
* CoE, *Convention on Cybercrime,* ETS 185, *Chart of signatures and ratifications*
* CoE, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, ETS 201, 25 October 2007
* CoE, Cybercrime Convention Committee, *Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, T-CY (2012)10, (2012)
* CoE, Cybercrime Convention Committee, *Assessment report – The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, T-CY(2013)17rev, (2014)
* CoE, Cybercrime Convention Committee, *Guidance Note # 3 Transborder access to data (Article 32)*, T-CY (2013)7 E, 3 December 2014
* CoE, Cybercrime Convention Committee, *Guidance Note #5 DDOS Attacks*, T-CY (2013)10E Rev, 5 June 2013
* Coe, European Committee on Crime Problems, Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters, *Case Law by the European Court of Human Rights of Relevance for the Application of the European Conventions on International Co-Operation in Criminal Matters*, PC-OC (2011) 21 REV 12, (2018)
* CoE, *European Convention on Extradition*, ETS 24, 13 December 1957
* CoE, *European Convention on Human Rights*, *Seventh Additional Protocol*, ETS 117, 22 November 1984

* CoE, *European Convention on the Suppression of Terrorism*, ETS 90, 27 January 1977
* CoE, *Explanatory Report to the Convention on Cybercrime*, ETS 185, 23 November 2001
* CoE, *Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime*, ETS 189, 28 January 2003
* CoE, *Project on Cybercrime Final Report*, ECD-567(2009)1, 15 June 2009
* CoE, *Recommendation No. R (89) 9 on Computer-related crime and final report on computer-related crime elaborated by the European Committee on Crime Problems*, 13 September 1989
* CoE, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology*, 11 September 1995
* CoE, *Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users*, CM/Rec (2014)6, 16 April 2014.
* CoE, *Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet*, MSI-INT (2014)08 rev6 Final, 10 December 2015
* CoE, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, ETS 182, 8 November 2001
* CoE, Venice Commission Opinion, *Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts*, n. 839/2016
* CoE, Venice Commission, Office for Democratic Institutions and Human Rights of the Organisation for Security and Cooperation in Europe, *Joint Guidelines on Freedom of Peaceful Assembly of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights* (2010)
* Common Market for Eastern and Southern Africa, *Cybersecurity Draft Model Bill* (2011)
* Commonwhealth of Indipendent States, *Agreement on Cooperation on Combating Offences related to Computer Information* (2001)
* Croatia, *Criminal Code*
* Czech Republic, *Criminal Code*
* Denmark, *Act n. 229/1985*
* East African Community, *Draft Legal Framework for Cyberlaws* (2008)
* Economic Community of West African States, *(Draft) Directive on Fighting Cybercrime* (2009)
* Economic Community of West African States, *Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS* (2011)
* Estonia, *Criminal Code*
* EU, *Accompanying Document to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical*

Information Infrastructure Protection 'Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience' – Summary of the Impact Assessment, COM(2009) 149 SEC(2009) 399, 30 March 2009

* EU, *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 19 July 2003
* EU, *Charter of Fundamental Rights of the European Union*, OJ C 326, 26 October 2012
* EU, *Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector*, C(2019) 2400 final, 3 April 2019
* EU, *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, COM/2004/0702 final, 20 October 2004
* EU, *Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, 28.3.2012 COM(2012) 140 final, 28 March 2012
* EU, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, [2000] COM/2000/0890, 26 January 2001
* EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, SEC(2009) 399, SEC(2009) 400, COM/2009/0149 final, 30 March 2009
* EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*, COM(2011)573, 20 September 2011,
* EU, *Consolidated version of the Treaty on European Union - Protocol (No 36) on transitional provisions*, OJ C 115 2008, 9 May 2008
* EU, *Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders*
  OJ L 239, 22 September 2000
* EU, *Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*, OJ L 138, 4 June 2009

* EU, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, OJ L 345, 23 December 2008
* EU, *Council Framework Decision 2002/465/JHA on Joint Investigation Teams*, OJ L 162, 20 June 2002
* EU, *Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism*, OJ L 164, 22 June 2002
* EU, *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, OJ L 69, 16 March 2005.
* EU, *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, OJ L 330, 9 December 2008.
* EU, *Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings*, OJ L 328, 15 December 2009
* EU, *Council Framework Decision of 24 October 2008 on the fight against organised crime (2008/841/JHA)*, OJ L 300, 11 November 2008.
* EU, *Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings*, OJ L 65, 11 March 2016
* EU, *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, OJ L 119, 4 May 2016
* EU, *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services,* OJ L 108, 24 April 2002
* EU, *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*, OJ L 335, 17 December 2011
* EU, *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, OJ L 218, 14 August 2013
* EU, *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*, OJ L 130, 1 May 2014

* EU, *Directive 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law*, OJ L 198, 28 July 2017.
* EU, *Explanations relating to the Charter of Fundamental Rights,* OJ C 303, 14 December 2007
* EU, *Joint action of 21 December 1998 98/733/JHA adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union*, OJ L 351, 29 December 1998,
* EU, *Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA,* [2010] COM(2010) 517 Final, OJ C 218, 23 July 2011
* EU, *Proposal for a Council Framework Decision on attacks against information systems*, COM(2002)173 final, OJ C 203E , 27 July 2002
* EU, *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, SEC(2010) 1122 final, SEC(2010) 1123 final, COM/2010/0517 final, COD 2010/0273, 30 September 2010
* EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* OJ L 119, 4 May 2016
* EU, *Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM(2008) 4488 final, OJ L 69/67, 16 March 2005
* EU, *Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, COM/2017/0474 final, 13 September 2017
* EU, *Report on the proposal for a directive of the European Parliament and of the Council on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA,* COM(2013)0042 – C7-0033/2013 – 2013/0023(COD), A7-0018/2014, 10 January 2014
* EU, *Summary Of The Impact Assessment Accompanying Document to the Proposal for a Directive of the European Parliament and of the Council on Attacks Against Information Systems, and Repealing Council Framework Decision 2005/222/JHA,* [2010] SEC(2010) 1123 Final, 30 September 2010
* Europol and European Union Agency for Cybersecurity, *Joint Statement - On lawful criminal investigation that respects 21st Century data protection*, 20 May 2016
* FR, *Code de Procédure Pénale*

* FR, *Code des postes et des communications électroniques*
* FR, *Code Pénal*
* FR, *Loi du 10 mars 1927 relative à l'extradition des étrangers*
* FR, *Loi n. 88-19 du janvier 1988 relative à la fraude informatique*
* FR, *Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*
* FR, *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*
* GER, *Bundeskriminalamtgesetz*
* GER, *Grundgesetz für die Bundesrepublik Deutschland*
* GER, *Informations- und Kommunikationsdienste-Gesetz* (1997)
* GER, *Poststrukturgesetz* (1984)
* GER, *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität* (1986)
* GER, *Strafgesetzbuch*
* GER, *Strafprozessordnung*
* Harvard Research in International Law, *Draft Convention on Jurisdiction with Respect to Crime*, (1935) 29 American Journal of International Law 435
* International Telecommunication Union / Caribbean Community / Caribbean Telecommunications Union, *Model Legislative Texts on Cybercrime* (2010)
* Israel, *Combating Criminal Organization Law* (2003)
* ITA, *Decreto Legge, 21 marzo 1978, n. 59 "Norme penali e processuali per la prevenzione e la repressione di gravi reati", convertito con modificazioni dalla L. 18 maggio 1978, n. 19*
* ITA, Camera dei Deputati, XI Legislatura, *Disegno di legge n. 2733, Presentazione del Ministro di Grazia e Giustizia G. Conso*
* ITA, *Codice di Procedura Penale*
* ITA, *Costituzione*
* ITA, *Decreto legislativo n° 216 del 29.12.2017*
* ITA, *Legge 29 luglio 1981, n. 406 "Misure urgenti contro la abusiva duplicazione, riproduzione, importazione, distribuzione e vendita di prodotti fonografici non autorizzati"*
* ITA, *Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"*
* ITA, *Proposta di Legge "Quintarelli", Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi,* 31 January 2017
* LAS, *Arab Convention on Combating Information Technology Offences* (2010)

* LAS, *Model Law on Combating Information Technology Offences* (2004)
* Latvia, *Criminal Code*
* OECD, *Recommendation of the Council Concerning Guidelines for the Security of Information Systems*, 26 November 1992.
* Organization of the American States, Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, *Concerns over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere*, Press Release R80/15, 21 July 2015
* Poland, *Police Act (Text No. 179)*
* Portugal, *Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime)*
* Romania, *Law 161/2003*
* Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security* (2008)
* Singapore, *Computer Misuse Act 2007*
* Spain, *Código Penal*
* Spain, Fiscalia General Del Estado, *Circular 2/2011 sobre la reforma del código penal por ley orgánica 5/2010 en relación con las organizaciones y grupos criminals* (2011)
* Sweden, *the Data Protection Act – Law n. 289* (1973)
* Swizerland, *Criminal Code*
* The Commonwealth, *Model Law on Computer and Computer Related Crime* (2017)
* The Netherlands, *Wetboek van Strafrecht*
* The Netherlands, *Wetboek van Strafvordering*
* The Philippines, *Presidential Decree n. 49* (1972)
* UK, *Serious Crime Act* (2015)
* UK, *Computer Misuse* (1990)
* UK, *Criminal Justice and Public Order Act* (1994)
* UK, *Forgery and Counterfeiting Act* (1981)
* UK, *Investigatory Power Act* (2016)
* UK, *Police and Criminal Evidence Act* (1984);
* UK, *Serious Crime Act* (2015)
* UK, *Terrorism Act* (2000)
* UK, *The Code for Crown Prosecutors* (2018)
* UK, *Theft Act* (1968)

* UN GA, Human Rights Committee, *Concluding Observation on the Sixth Periodic Report of Italy*, CCPR/C/ITA/CO/6, 28 March 2017
* UN GA, Human Rights Committee, *General Comment N. 34 (Article 19 ICCPR)*, 12 September 2011
* UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, 17 April 2013
* UN GA, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32, 22 May 2015
* UN GA, Human Rights Council, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai*, A/HRC/20/27, 21 May 2012
* UN GA, Human Rights Council, *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, A/HRC/23/40, 17 April 2013
* UN GA, Human Rights Council, *Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,* A/69/397, 234 September 2014
* UN GA, Human Rights Council, *The right to privacy in the digital age*, A/HRC/34/7, 27 February 2017
* UN GA, *Report of the Ad Hoc Committee established by General Assembly Resolution 51/210 of 17 December 1996*, Sixth session, A/57/37 1 February 2002
* UN GA, *Resolution 1962 (XVIII), Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, 13 December 1963
* UN GA, *Resolution 55/63, Combating the criminal misuse of information technologies*, A/RES/55/63; 4 December 2000
* UN GA, *Resolution 56/121, Combating the criminal misuse of information technologies,* A/RES/56/121, 19 December 2001
* UN GA, *Resolution 64/2011, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical infrastructures*, A/RES/64/211, 17 March 2010
* UN GA, *Resolution 51/210, Measures to eliminate international terrorism*, A/RES/51/210, 17 December 1996
* UN GA, *Resolution 71/199, The right to privacy in the digital age*, A/RES/71/199, 25 January 2017
* UN GA, *United Nations Report of the International Law Commission*, A/61/10, Annex E, 11 August 2016

* UN, *Convention against Transnational Organized Crime and the Protocols Thereto*, UN GA Resolution A/RES/55/25, 15 November 2000
* UN, *International Convention for the Suppression of the Financing of Terrorism*, UN GA Resolution A/RES/54/109, 9 December 1999.
* UN, *International Convention on the Elimination of All Forms of Racial Discrimination*, UN GA Resolution 2106 (XX), 21 December 1965
* UN, *International Covenant on Civil and Political Rights*, UN GA Resolution 2200A (XXI), 16 December 1966
* UN, *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*, UN GA Resolution A/RES/54/263, 25 May 2000
* UN, *Rome Statute of the International Criminal Court*, UN A/CONF.183/9 (1998)
* UN, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, UN GA Resolution 2222 (XXI), annex, 19 December 1966
* UN, Working Group on Internet Governance, *Report of the Working Group on Internet Governance*, 2005
* US, 95th Congress, *Congressional Records* (Vol. 123, No. 111, 1977)
* US, American Law Institute, *Restatement (3rd) of Foreign Relations Law* (1987)
* US, Committee on Governmental Operations, the 95th Congress 1 Session, *Staff Study of Computer Security in Federal Programs* (United States Senate 1977)
* US, *Computer and Communications Security and Privacy: Hearings Before the Subcommittee on Transportation, Aviation, and Materials of the Committee on Science and Technology*, U.S. House of Representatives, Ninety-eighth Congress, First Session (1983)
* US, *Computer Software Copyright Act* (1980)
* US, *Model Penal Code*
* US, *Privacy Act* (1974)
* US, *United States Code*
* US, *West Virginia Penal Code*