INTERNATIONAL
HELLENIC
UNIVERSITY

# *Using Social Networks for Law Enforcement. The Hellenic Paradigm.*

**Christos V. Antonoudis**

SID: 3307180001

**SCHOOL OF SCIENCE & TECHNOLOGY**

A thesis submitted for the degree of

***Master of Science (MSc) in Cybersecurity***

January, 2021

Thessaloniki – Greece

| | |
|---|---|
| Student Name: | Christos V. Antonoudis |
| SID: | 3307180001 |
| Supervisor: | Prof. Komninos Komnios |

I hereby declare that the work submitted is mine and that where I have made use of another’s work, I have attributed the source(s) according to the Regulations set in the Student’s Handbook.

January 2021

Thessaloniki - Greece

# Abstract

This dissertation was written as a part of the Master of Science (MSc) in Cybersecurity at the International Hellenic University, during the academic year 2018-2020.

In the Introductory Chapter, the general concept of Social Media Platforms will be introduced, accompanied by a brief explanation on the importance of users' data utilization by Law Enforcement Authorities.

The thesis is separated in five (5) chapters. In chapter 1, the categories and forms of Social Media Platforms are analyzed. Chapter 1 focuses on defining social media, along with providing a historical preview of the most known social networks. Moreover, the terms related to cybercrime and the roles of the police agencies that investigate it, are presented.

Chapter 2 gets into a deep analysis of the relationship between social media and users' data. A preview on how the legislation regarding the protection of people's personal data changed through time, is unraveled. Additionally, the definition of the term "Big Data" is mentioned, along with a brief description of the implemented data storage mechanisms.

In chapter 3, the most common types of cybercrime committed on social media, are thoroughly examined. Furthermore, the collaboration between Law Enforcement Authorities and Social Media Platforms is studied, including the requesting for disclosure of users' data, along with any other applied investigating practices.

Chapter 4 heads inside a Law Enforcement Authority. Real time scenarios of criminal cases and interviews of high-ranking law enforcement agents are unfurled, accompanied by a presentation of the Hellenic Cyber Crime Unit paradigm.

Chapter 5 proposes the development of a new intelligence database, which may ameliorate the collaboration between Law Enforcement Authorities and Social Media Platforms. In addition, several recommendations are presented, concerning the improvement of the services of the Hellenic Cyber Crime Division.

The "Conclusions" chapter evaluates in brief what we have learned from the whole thesis.

Lastly, the "Discussions" chapter, deals with the widely discussed concerns on the subject of usage of social media users' data by the police.

Christos V. Antonoudis

January 2021

# Acknowledgement

At this point, I would like to express my gratefulness for the people who altruistically provided their assistance and support during the production of this thesis. Most of all, I would like to thank my supervisor, *Prof. Komnios Komninos*, who enlightened me through all this period, along with my friends, family and colleagues that kept me going. I would also like to thank the people of the Hellenic Police Headquarters, who granted me access to the archives of the Cyber Crime Subdivision of Northern Greece. Lastly, I would like to express my gratitude to the high-ranking police officers of the Cyber Crime Subdivision of Northern Greece, who spent their personal time to assist me with the thesis.

Christos V. Antonoudis

January 2021

# Contents

# Introduction

It is common sense that the year 2020 has been a major setback. Pandemic, quarantines, natural disasters, wars in the western civilization, etc. But this is not the first time that planet Earth faces such crises. Although it may seem a distant past from today' s community, people have suffered from these phenomena repeatedly. The only aspect that is different nowadays may be stated in just one word. *Information*. Information is power. Every single person has the power to gain knowledge of what is happening right now, across the entire planet. People can interact with each other, make all kinds of transactions, exchange thoughts, or even create intimate relationships. Even though, Internet has provided this kind of power, nothing could be achieved without the existence of an intermediate which would congregate all this information. This intermediate has a name, and it is called *Social Media Platform (SMP).*

Social Media Platforms present their users with a unique opportunity. To visit a virtual world and coexist with other people. The possibilities that these platforms provide are endless. A person from France may interact with another person from China through "Tinder" and form a romantic relationship. A developer from United Kingdom could find his/her dream job in the U.S.A. through "LinkedIn". A Greek patient, having a rare disease, could join a group of people facing the same challenges and learn alternative methods of healing; just by searching through "Facebook". It may not sound that fascinating for someone who has been raised with this kind of technology. But what would people do if social media just seized to exist? Could they handle this kind of loss?

Communication and information are the two pillars which established the foundations of our "Information Society" era. Politics, heath, relationships, business, education; everything is based on these two pillars. Social media were created to facilitate them. Providing that they are used with righteousness and under the applicable law, society can only benefit from them.

Nonetheless, social medias' users should not get carried away. As technology progresses, criminals' methods do to. People tend to believe everything that is presented to them, without any further seek for knowledge. Cyberspace is no exception. In the next few chapters, a detailed analysis on how these platforms function will be unraveled. In every single service provided by the platforms, there will always be a penetrator who will try, and many times achieve to exploit it. This criminal act may be against a simple user, a multinational company or even a public institution.

Consequently, the wide spread of Social Media Platforms renders as a necessity, the establishment of *Law Enforcement Authorities (LEAs)*, specialized in investigating cybercrime. Each country has its own specialized police forces. They are called *"Cyber Crime Units" (CCUs).* Depending on the public sector they serve, they require different kind of specialized knowledge (forensics examination, networking, cybersecurity, malware analysis, etc.). At this point it is important to clarify that CCUs are not responsible for *Internet Governance.* People may think that what a cybercrime agent does, is monitor the cyberspace traffic and prevent everything that may cause damage. But this is not entirely accurate.

Law Enforcers involved in cybercrime, are burdened with the responsibilities of investigating crimes that take place inside the cyberspace, not securing its data traffic. Although preventing cyber criminality would resolve every probable issue, it is a method that is not applied in reality. Identify theft, child sexual abuse/exploitation, fraud related cases, are merely some of the crimes related to their investigations. The major challenge of a CCU, is to find the legitimate means in order to discover the unknown perpetrators' personal information. To resolve this problem, social networks came to their aid.

In order to gain access into a social network and reap its benefits, a user must create a profile. Through the registration process, users provide several personal data. Registered e-mail, contact information, full name, or username, are only some of them. Moreover, under their terms of services, social media store users' networking information (IP addresses, timestamp, time zone). Many of them may also store, sent or received files (photographs, videos, messages, etc.). Although the average user may not understand the importance of this information, LEAs can find them very useful.

What is dubious about this method, is at what point CCUs are justified to request and receive a user's personal data by Social Media Platforms. Is it legitimate to use them in penal proceedings, or may it cause throwbacks? Many journalists, authors and academics have tried to provide a justified answer. This thesis will try to present a different angle and introduce the standpoint of the people who are in the front line of the war against cybercrime.

# 1 Introduction to the concepts of Social Media Platforms and Cybercrime

## 1.1 What Social Media Platforms are – Web 2.0.

There have been many given definitions regarding a Social Media Platform. In «How the World Changed Social Media», Miller/ Costa et al. describe social media as *"the colonisation of the space between traditional broadcast and private dyadic communication, providing people with a scale of group size and degrees of privacy that we have termed scalable sociality."* [1]. What the authors try to explain is that SMPs were created to fill the gap between public forums and private conversations. Before their existence, there were many websites that provided public group chats, or plenty of applications via which someone could chat with a friend. What is different after the introduction of social media is that they have provided a means, through which private communications were finally reachable through group communication programs.

Merriam – Webster's online dictionary defines social media as *"forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)"* [2]. This definition aims to describe the possibilities that SMPs provide, in more general terms.

Although "social media" is the widely accepted term for social networking platforms, Internet users should not be confused. It must be clarified that Social Network Sites (SNSs), such as "Facebook", "Twitter", etc., are just a certain type of social media. SMPs can be categorized into six groups:

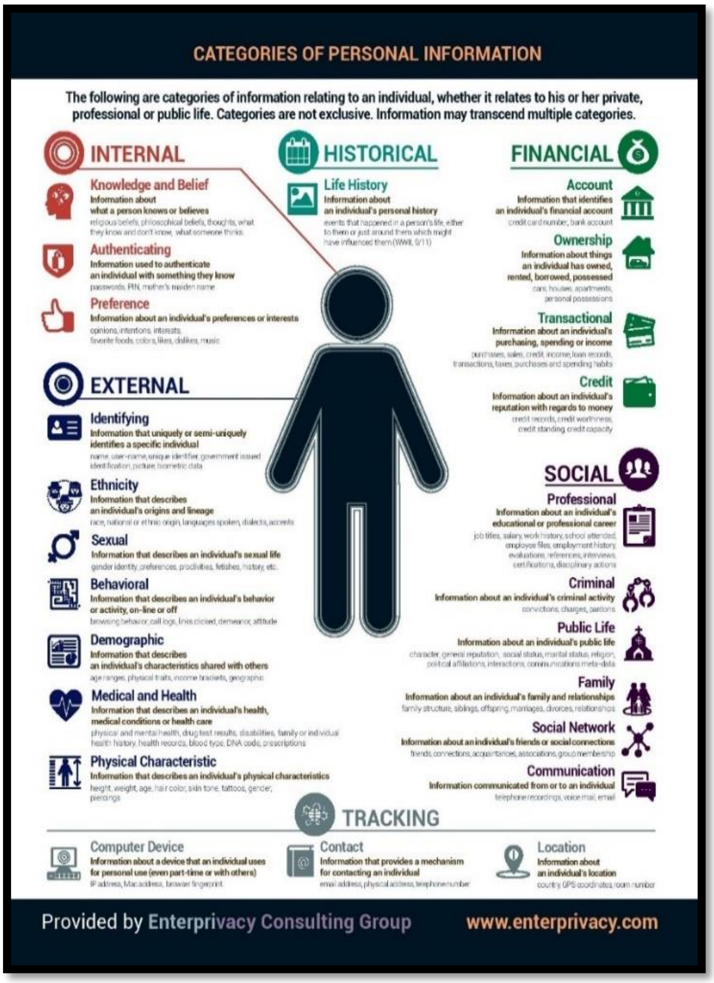
1. *Collaborative projects (e.g., "Wikipedia"),*
2. *Blogs, including microblogs (e.g., "Twitter"),*
3. *Content communities (e.g., "YouTube"),*
4. *Social networking sites (e.g., "Facebook", "LinkedIn"),*
5. *Virtual game worlds (e.g., "World of Warcraft"), and*
6. *Virtual social worlds (e.g., Second Life).* [3]

Nevertheless, as the majority of people use Social Networking Sites, they do not understand the differences between SMPs and their basic characteristics. Let us take a closer look to SNSs and try to understand their importance.

What are Social Networking Sites? The most adequate definition is the one given by Danah M. Boyd, a Principal Researcher at Microsoft Research and the founder of Data & Society, who tried, and to a great extent achieved to define and characterize social media. According to her, *"We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site."* [4]. By giving this definition, the author has listed the three stages that every user must repeat in every social network platform.

Though the registration phase of a SNS, the user is asked to create a profile before beginning his/her virtual experience. S/He is provided with a form, usually containing a series of questions, which vary from date of birth and full name (external identifying personal data) to preferred hobbies or current employment (social personal data), as demonstrated in **Figure 1**. Another common practice is the upload of a personal photo, which will be widely visible and is requested so as to identify a single user, among many others. Depending on the SNS, the user must also answer different kinds of questions. Although some of them may only ask for an email address or a registered phone number, some others need profoundly more personal information to complete the desirable profile. At the end of this process, a profile is generated through the series of questions and a unique identity for the user in question is produced.

The basic concept of a SNS, is to connect its users to the virtual world. Thus, after the creation of the profile, the "netizens" *(i.e., Internet users* [5]*)* are encouraged to browse the platform and find others, with whom they are able to share a vague but promising connection. The kind of connection varies from ethnicity or religion, to preferred sport or music interests. These relationships/connections are characterized as "Friends", "Followers", "Subscribers", etc. They differ from one SNS to another and they represent the form of connections that their designers wish to establish. What is also different through each SNS, is the choice of making a "friendship". Usually this choice is bidirectional, meaning that each user is given the option of being “Friends” with another user or contrariwise, block him/her.



CATEGORIES OF PERSONAL INFORMATION

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.

INTERNAL

Knowledge and Belief
Information about what a person knows or believes
religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks

Authenticating
Information used to authenticate an individual with something they know
passwords, PIN, mother's maiden name

Preference
Infomation about an individual's preferences or interests
opinions, intentions, interests, favorite foods, colors, likes, dislikes, music

EXTERNAL

Identifying
Information that uniquely or semi-uniquely identifies a specific individual
name, user-name, unique identifier, government issued identification, picture, biometric data

Ethnicity
Information that describes an individual's origins and lineage
race, national or ethnic origin, languages spoken, dialects, accents

Sexual
Information that describes an individual's sexual life
gender identity, preferences, proclivities, fetishes, history, etc.

Behavioral
Information that describes an individual's behavior or activity, on-line or off
browsing behavior, call logs, links clicked, demeanor, attitude

Demographic
Information that describes an individual's characteristics shared with others
age ranges, physical traits, income brackets, geographic

Medical and Health
Information that describes an individual's health, medical conditions or health care
physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions

Physical Characteristic
Information that describes an individual's physical characteristics
height, weight, age, hair color, skin tone, tattoos, gender, piercings

HISTORICAL

Life History
Information about an individual's personal history
events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)

FINANCIAL

Account
Information that identifies an individual's financial account
credit card number, bank account

Ownership
Information about things an individual has owned, rented, borrowed, possessed
cars, houses, apartments, personal possessions

Transactional
Information about an individual's purchasing, spending or income
purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits

Credit
Information about an individual's reputation with regards to money
credit records, credit worthiness, credit standing, credit capacity

SOCIAL

Professional
Information about an individual's educational or professional career
job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions

Criminal
Information about an individual's criminal activity
convictions, charges, pardons

Public Life
Information about an individual's public life
character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data

Family
Information about an individual's family and relationships
family structure, siblings, offspring, marriages, divorces, relationships

Social Network
Information about an individual's friends or social connections
friends, connections, acquaintances, associations, group membership

Communication
Information communicated from or to an individual
telephone recordings, voice mail, email

TRACKING

Computer Device
Information about a device that an individual uses for personal use (even part-time or with others)
IP address, Mac address, browser fingerprint

Contact
Information that provides a mechanism for contacting an individual
email address, physical address, telephone number

Location
Information about an individual's location
country, GPS coordinates, room number

Provided by Enterprivacy Consulting Group www.enterprivacy.com

***Figure 1****: The different categories of Personal Information*

As previously mentioned, each “cybernaut” *(i.e., “a netizen”* [6]*)* has his/her own “Friends” list. The key to this feature, is the public view of each user’s connections. Plenty SNSs allow every user to check another’s “Friends” list, while some others demand a prior connection between two “netizens”, according to their enabled privacy settings. Viewers are partially allowed to go through the entire “network graph”, through another’s “Friends” list. Although it may seem quite worthless for the average user, it is a valuable tool for the person who needs to dig inside the SNS, or even for the expansion of the Net itself.

Another remarkable attribute of SNSs is the ability to share content. The majority of social media allow their users to exchange messages, share videos and photographs, or even be a part of real-time videos. Messaging is divided in two categories: a) direct messaging, and b) content responding or *“comments”*. Undoubtedly, sharing any kind of content is the main goal of the founders of each platform. Communication, which resolves to the creation of a community inside a virtual world.

Social Media Platforms have altered the ways of the World Wide Web (WWW). Before 2005, when the vast thriving of SNSs occurred, Internet websites functioned in a more passive manner. There were no connections between creators and viewers. In 2000, the

Internet was purely used for the provision of news and historical information and consequently caused the crisis of its economy. Web 2.0, which is the concept of the next – generation Internet technologies (interactive Internet) [7], is highly dependable with social media. In reality, SNS technologies were the founders of WWW's new era. The role of the "average user" has seized to exist and gave its place to the "data distributor". The enabling of communication along with the provision of content (live or already existed data), have turned the "netizen" into a contributor to Internet's content. Broadly speaking, "virtual communities" promote the expression of thoughts, opinions, or beliefs of any kind [8]. The new applications that SNSs featured, along with the interactive capabilities they provided, proclaimed the need for individual users to play a significant role in the expansion of WWW. Thus, anyone may effortlessly jump to the conclusion, that the induction of SNSs is of great importance. To make things even simpler: is there anyone who does not have a profile in any Social Media Platform?

## 1.2 Which are the most famous Social Media Platforms and how they operate

Although all major SMPs made their appearance around 2005, the very first social network was introduced to the public in 1997 and its name was "SixDegrees.com". Surely, many others existed prior to it, like "classmates.com" or "match.com", but none of them combined all the basic characteristics of a SNS. "SixDegrees.com" successfully enabled the features of creating profiles, producing a "Friends" list and, in 1998, to surf another user's "Friends" list. The features were presented as electronic bulletin boards, e-mails, and online messages. The concept behind this SNS was to allow its users, who were previously unknown to each other, to connect and interact through messaging (**Figure 2**). Although it attracted many users, "SixDegrees'" services were closed in 2000.

Going forward to year 2001, "Wikipedia" is being launched. As stated in its website, *"Wikipedia is an online free-content encyclopedia project helping to create a world in which everyone can freely share in the sum of all knowledge"* [9]. "Wikipedia's" website is supported by "Wikimedia Foundation" and it is presented as a *"free-content online encyclopedia project"*. It allows the users to voluntarily add content to the website's databases (DBs), resulting in the creation of a gigantic online library. Every page consists of several links that cite additional articles, regarding the referred topic. "Wikipedia" stores users' personal information, such as IP addresses and public contributions [10].

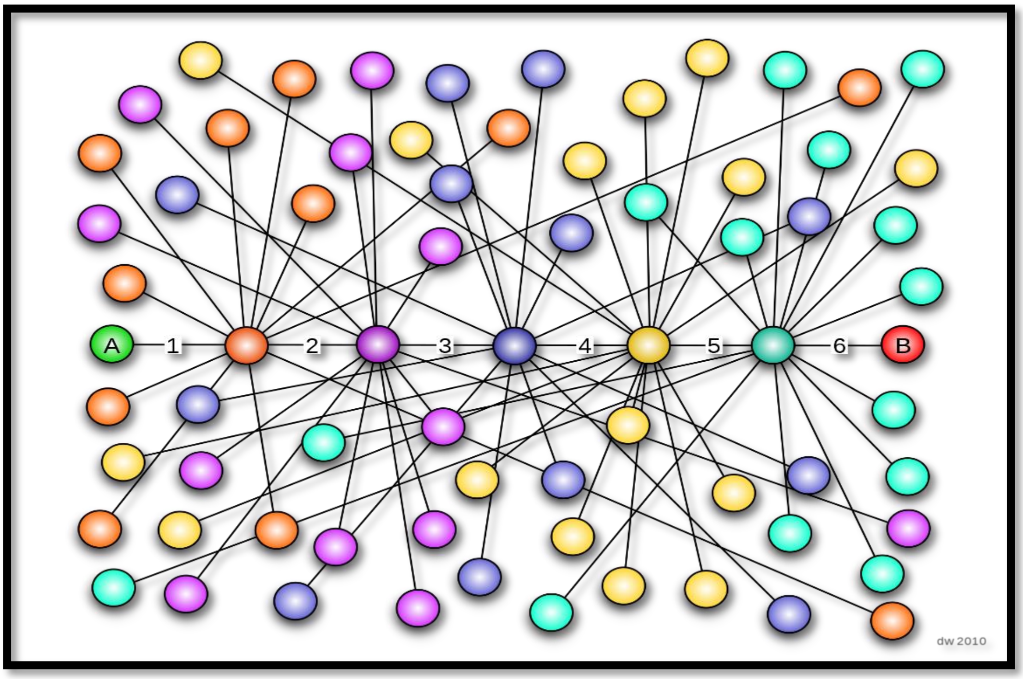


***Figure 2**: Six Degrees of Separation*

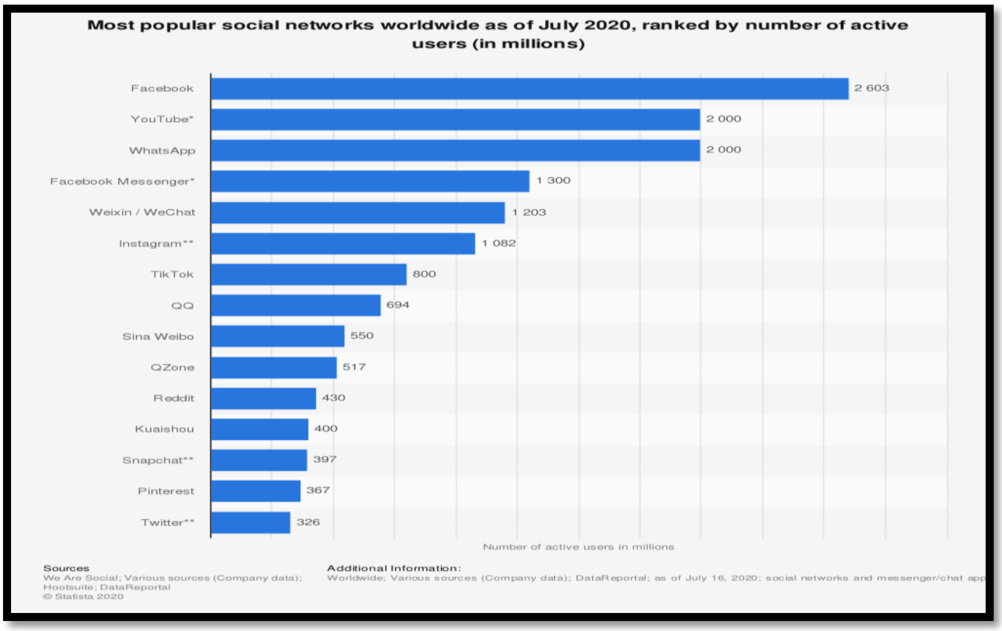
The year is 2003 and “LinkedIn” introduces itself to the public. It is a SNS, created for professionals who seek to publicly display their work experience [3]. “LinkedIn” could easily be described as an online Curriculum Vitae (CV). This SNS is allegedly the largest “professional network” existing in 2020. As previously mentioned, it is highly recommended for professionals who either seek for a job opportunity or enquire about a work vacancy. It can be easily understood that as users upload their personal CVs, this SNS stores all kind of a user’s personal data.

In the same year, another SNS was created. Its name was “MySpace”. In 2006, “MySpace” overtook “Google” and became the most visited SNS in the U.S.A. Although “MySpace” is not that commonly used nowadays, it made a huge impact in today’s networking society.

Another important part of SMPs is “content communities” [11]. Websites like “4chan”, “YouTube”, “Pinterest” and “Reddit” allow their users to share multimedia content with each other. The type of content varies from photographs and videos, to articles and short stories. It is important to mention that these “content communities”, not only store personal information provided by the users through the registration phase, but they also store, and some time own, the content that the users upload. Thus, it is of high importance that the users read the “Terms of Service” of each SMP and not just use it as a storage location for their uploaded media.

As it has been already mentioned, “YouTube” is considered a “content community”. This SMP was founded in 2005 but was eventually purchased in 2006 from one of the greatest technology companies, “Google LLC”. Ever since, “YouTube” is considered as one of “Google’s” subsidiaries. Despite the fact that “Google” is widely recognized for its search engine, it is considered as one of the most widespread online communities across the planet. All services provided by “Google” (Maps, Search Engine, Gmail, Chrome, etc.) may be integrated in one single account, created by the user in question. Categorically, “Google” cannot be presented as a SMP. Nevertheless, some of its services’ characteristics are familiar to SMPs’ attributes, such as messaging through “Gmail” or creating a “Friends” list.

Going forward to 2004, the users encounter “Facebook” for the first time. In the beginning it was introduced to Harvard students. In 2005, “Facebook’s” network expanded to high schools and it was until 2006, that its founders provided its services to the public. “Facebook” could easily be provided as an example for defining a SNS. It allows its users to create a uniquely identified profile, roam through the network, add virtual friends and check other users’ “Friends” list. As shown in **Figure 3**, “Facebook” is the most popular SNS in 2020, ranked by number of active users. It can be easily comprehended that “Facebook” may store a significant amount of a user’s personal information, either through the registration phase, or by the content shared among users or even through the platform’s messaging feature.



Sources
We Are Social; Various sources (Company data); Hootsuite; DataReportal
© Statista 2020

Additional Information:
Worldwide; Various sources (Company data); DataReportal; as of July 16, 2020; social networks and messenger/chat app

*Figure 3: Most popular social networks worldwide as of July 2020, ranked by number of active users (in millions)*

Along with “Facebook”, Facebook Inc. owns another highly influential SNS. “Instagram” was originally launched in 2010 and it is proclaimed to be an application between “content community” and a SNS. “Instagram” is a modern medium, which allows its users to capture their lives’ moments and share them with their “Friends” (i.e., “Followers”) [12]. This SNS also enables messaging among users, through “direct messaging”. “Instagram” is one of the most rapidly growing SNSs, as in just ten years of existence, has more than one billion registered users (Figure 3). Although “Instagram” is highly widespread to the public, it has been the subject of criticism, most importantly for the improper material uploaded by its users.

“Twitter” is yet another major SMP, proclaimed to be a SNS. The website - application allows its registered users to post content and interact through messages, called *“tweets”*. The fact that these services are only provided for registered users, while unregistered ones can only read the “tweets”, is notable. “Twitter” was originally launched in 2006 and it is owned by the company “Twitter Inc.” [3]. “Twitter” also stores a considerable amount of information regarding its users, such as account history, account activity, associated devices, etc. [13].

Despite the numerous digital platforms existing in cyberspace, this thesis could not omit one of 2020’s trends. “Tik Tok” is a SNS, usually downloaded as an application for i-Phone Operating Systems (iOS) or Androids and was developed in order to create an “online entertainment community” [14]. “Tik Tok” was launched in 2017 in China, but became available to the rest of the world, after its amalgamation with “Musical.ly”, in 2018. By examining Figure 3, it can easily be understood that in only two years, “Tik Tok” managed to become one of the most famous SNSs worldwide.

Last but not least, “dating apps” should be acknowledged as one of the most unique categories of SMPs, as they have a major impact on establishing today’s socializing culture. “Tinder”, “Bumble”, “PlanetRomeo” and “The League” are some of the sites that belong to this special category. In the next chapters, the importance of “dating apps” will be manifested, since penetrators tend to frequently use them with the intention to find their “sitting ducks” *(i.e., easy targets or victims* [15]*)*. Thus, their impact in acquiring users’ data for investigating cyber criminals is signified.

## 1.3 General concepts of cybercrime – Historical Preview

Along with its provided financial and interactive benefits, cyberspace offers an ideal visual environment for the thriving of criminality [16]. While offences committed through personal interaction have reached their zenith internationally, cybercrime is introduced as an alternative method of criminality. Theft, bullying, sexual abuse, terrorism are crimes committed every day worldwide. The different possibility that cyberspace provides is *anonymity*. Instead of executing these violations through interpersonal contact, a criminal may stay in his/her apartment and act harmfully against a person living on the other side of the planet. Additionally, if s/he possesses the proper knowledge and the proper tools, s/he may destroy all evidence that could possibly lead to his/her true identity.

Historically in 1994, as the need for protection against cybercrime increased, United Nations formed a manual, in order to define it, designate its common traits and build the first line of defense against offenders. According to the manual, the most usually committed crimes on cyberspace were: (i) fraud by computer manipulation, (ii) computer forgery, (iii) damage to or modifications of computer data or programs, (iv); unauthorized access to computer systems and service, and (v) unauthorized reproduction of legally protected computer programs [17].

Moving forward to 2001, the Convention on Cybercrime [18], held in Budapest, provided a list of all related criminal offences. Namely, these offences are: (i) – Offences against the confidentiality, integrity and availability of computer data and systems, (ii) – Computer-related offences, (iii) – Content-related offences and (iv) – Offences related to infringements of copyright and related rights [19].

The fact that any research, academical writing or guide regarding cybercrime, integrates a definition of the term is well known. According to EC3 *(see below, p. 14)*: *"Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)"* [20]. Moreover, another given definition refers to the term cybercrime as: *"crime that is enabled by, or that targets computers"* [21]. By comparing each approach, the reader may come to a very significant conclusion. Although, the words of the definitions change, the concepts that surround the term itself, remain the same. Thus, this thesis may not try to define cybercrime *per se*. On the contrary it will present in plain terms the surrounding concepts of the term, as well as the related offences.

The basic terms related to a cybercrime are: “computer system”, “computer data”, “service provider” and “traffic data”. As defined in the Convention on Cybercrime:

1. *“computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data”,*
2. *“computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”,*
3. *“service provider means:*
    i. *any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and*
    ii. *any other entity that processes or stores computer data on behalf of such communication service or users of such service” and*
4. *“traffic data means 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.”* [18].

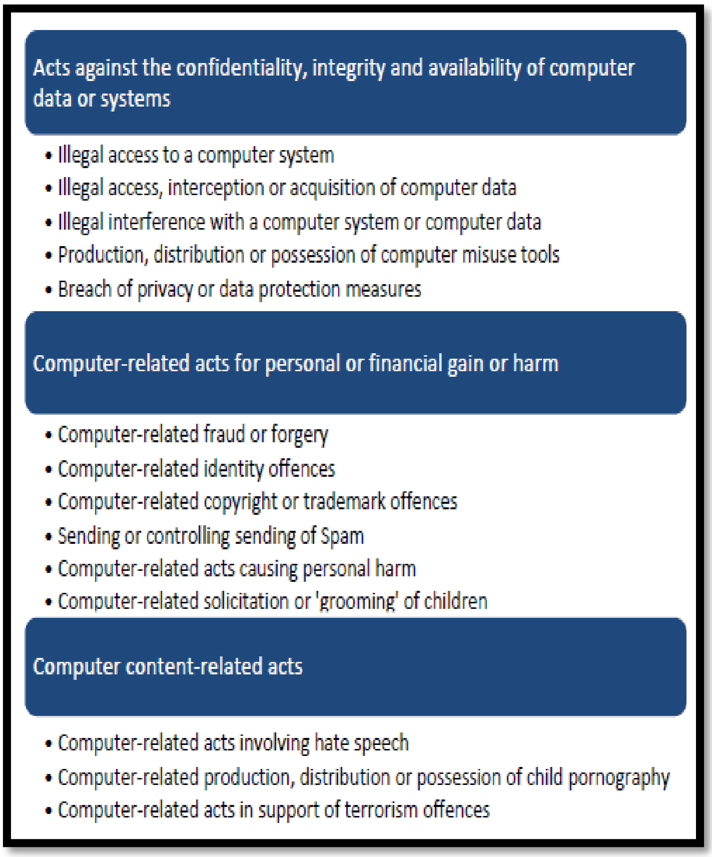
Another substantial term that should be included among the rest, is “network”. A “network” is *“an interconnection between two or more computer systems”* [3]. Before moving on to listing criminal offences related to cybercrime, an analysis of the surrounding terms is necessary.

A “computer system” can be any kind of device, or group of devices, containing both software and hardware, resulting in an *“automatic processing of data”* [3]. Automatic processing refers to a process that does not need human handling. It should be noted that since technology changes rapidly, a specific list of “computer systems” does not exist, as any technology non-registered in the list, would fall outside the provided legislative provisions.

According to the ISO standard [22], *“data is a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing”*. Practically, “computer data” as a cybercrime related term, is any information stored in a physical medium (e.g., USB flash drive), a computer system’s memory or a cloud service, that can be automatically processed by the computer system in question.

Hence, the inclusion of the term *"program"*, as the means which automatically processes data, becomes quite clear.

To conclude the basic concepts of cybercrime, it is considered unavoidable to enumerate the criminal acts constituting it. As stated in the Convention on Cybercrime, offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, and content-related offences, consist of the criminal acts depicted in **Figure 4** [16].



Acts against the confidentiality, integrity and availability of computer data or systems

- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal interference with a computer system or computer data
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

Computer-related acts for personal or financial gain or harm

- Computer-related fraud or forgery
- Computer-related identity offences
- Computer-related copyright or trademark offences
- Sending or controlling sending of Spam
- Computer-related acts causing personal harm
- Computer-related solicitation or 'grooming' of children

Computer content-related acts

- Computer-related acts involving hate speech
- Computer-related production, distribution or possession of child pornography
- Computer-related acts in support of terrorism offences

***Figure 4**: Categories of Cybercrime*

Namely, the related offences of each category, according to the Council of Europe are:

1. Offences against the confidentiality, integrity and availability of computer data and systems:
   i. Illegal access,
   ii. Illegal interception,
   iii. Data interference,
   iv. System interference,
   v. Misuse of devices.

2. Computer-related offences:
    1. Computer-related forgery,
    2. Computer-related fraud.
3. Content-related offences:
    1. Offences related to child sexual abuse/exploitation.
4. Regarding offences associated with infringements of copyright and related rights, the Council of Europe assigned each member state with the responsibility of legislating the right and proper law, in order to establish the related criminal offences, under its domestic legislation [21].

## 1.4 Cyber Crime Units – Operation, Training and Public Interaction

Before heading deep inside the core of the thesis, it is inevitable to briefly discuss the role of a Cyber Crime Unit. CCUs are specialized Law Enforcement Authorities and are considered to be the most significant part of disrupting and preventing cybercrime. Where local police's jurisdiction ends, CCUs perform their duties in order to uncover the unknown perpetrator's true identity.

As stated in the Introductory Chapter, Internet has offered many advantages in modern communication and interaction. But whenever society finds a way to make life easier for its individuals, there will always be a percentage of the population that will try to exploit these merits, to its own profit. Assuredly, crime had existed long before Internet's birth. However, the ushering of cybercrime proclaimed the need of implementing special techniques, in the war against criminals.

Whereas the traditional model for police investigations consists of hands-on approach on physical evidence, crime scene examination and witnesses' statements, the foundation of CCUs introduced a vast variety of new investigative techniques. Social engineering, computer forensics, analyzing traffic data, malware analysis, etc. are some of the methods that gave a significant boost in the stoppage of criminality.

Evidence regarding cybercrime acts is usually in digital form. Computer and traffic data may be stored and transferred both physically and digitally. Their form varies, from computer files to metadata and logs [16]. Although physical medium storages can be acquired through traditional police investigation, their analysis is usually performed by police agents in technologically suitable laboratories, by using digital forensics. On occasions where prevention of crime is exceedingly demanded, police agents cooperate with other private entities to offer solutions for potential problems; for instance, the analysis of an already deployed malicious code (malware analysis) and the free distribution of its *decryptor key*, to the public. More precisely, analyzing a user's log data, who used his/her social media account to act harmfully against other users, is a case that demands at least the fundamental networking skills and knowledge.

Nonetheless, there are times when exceptional expertise or technical support may not come in handy. Therefore, LEAs utilize SMPs for various reasons. For investigative purposes as, for example, focusing on a specific individual or its network in order to obtain more information about him/her, or for verifying the commitment of a particular criminal activity. Additionally, collecting evidence regarding the criminal actor himself/herself or his/her current whereabouts.

Undeniably, the leading International Police organization battling against cybercrime, is *INTERPOL* **(Figure 5)**. Since 1980, the institution performs both as an operator and as an instructor. Apart from advising the public regarding cybercrime's new trends, *INTERPOL Cybercrime Directorate*, in cooperation with member states' LEAs, private sectors organizations and Computer Emergency Response Teams (CERTs), has coordinated several international operations [23]. Moreover, INTERPOL has affiliated with a variety of member countries' Police Agencies, in order to train the police personnel and develop cyber skills, knowledge and technical abilities [24].

***Figure 5**: INTERPOL*

In a more regional approach, *EUROPOL* **(Figure 6)** has established an exquisite technical Agency, in response to cybercrime, called *EC3*. EC3 was built by EUROPOL in 2013, and its aim is to protect European citizens against criminal acting through Internet. The Agency performs in various ways, like creating joint operations with its member states (J-CAT). Furthermore, EC3 organizes plenty conventions, along with a series of training seminars, in order to ensure that law enforcement agents are kept up to date, depending on their fields of expertise. Last but not least, EC3

***Figure 6**: EUROPOL – EC3*

annually issues a report (called IOCTA) regarding key findings, threats and advancements in cybercrime [25].

Among many other LEAs that investigate cybercrime, *FBI's Cyber Division* **(Figure 7)** is one of the most innovative. Along with its trained cyber squads (Cyber Action Team) and the established partnerships with both private and public sector, in order to prevent crimes against U.S.A.'s networks and infrastructure, the bureau has launched *IC3* and *iGuardian*, with which the public can interact directly with the Agency and file their complaints, regarding potential or ongoing cybercrimes [26]. In addition, FBI issues its own annual report, based on the records of IC3, called Internet Crime Report.

FEDERAL BUREAU OF INVESTIGATION
iC3
INTERNET CRIME COMPLAINT CENTER

***Figure 7****: FBI – IC3*

Since we have discussed the most prominent CCUs worldwide, it would be unacceptable to disregard the importance of the *European Network and Information Security Agency* (*ENISA* – **Figure 8**). Even though ENISA is more of an EU's organization, rather than a Law Enforcement Authority, it has significantly contributed to the war against cybercrime. The organization annually proposes its strategic objective [27], through which it wishes to achieve *"a high common level of cybersecurity across Europe"*. Historically, it was established in 2004 and it still cooperates with all member states and bodies of EU. All in all, ENISA's initiative includes informing the public regarding potential cybercrime incidents, training EU cybercrime agencies about the proper means of investigation and consulting the private sector on ways to achieve absolute cybersecurity.

***Figure 8****: ENISA*

It is highly important to clarify that cybercrime investigations include all kind of techniques. A cybercrime officer's investigation is typically directed in acquiring information or examining the data already procured. Usually, acquiring information is an obligation of the "first responder". The investigator, who this obligation is assigned to, ought to preserve the digital and physical evidence, determine the source of the cyber event and limit the perpetrator's damage. Nevertheless, acquisition of data can be obtained through numerous "intelligence" techniques, which will be unraveled in the following chapters [28].

Following the stage of information acquisition, the investigation involves examination of data. Examination is accomplished either through automated software or by-hand. According to the level of expertise required, it is either completed by special examiners, called forensic examiners, or by traditional investigators.

The most difficult part of a cybercrime investigation is the compilation of evidence. Even though evidence in an interactive crime can be effortlessly found, the limits that virtual worlds pose are binding. In traditional crimes, a victim's testimony is the first piece of acquired evidence, along with the provision of several additional material. To aid this investigation, SMPs and hosting companies, may likewise provide the substantial data, which could possibly lead to the identification of an unknown perpetrator.

As society has reached the "Information Era", the use of SMPs has grown into a necessity for everyone. The Internet activity revolved around them leads to the fact that people have merged SMPs into their everyday lives. As criminal activity can be represented as a human deed, it cannot be excluded. Subsequently, as law enforcers exist in order to prevent such acts from taking place, the fact that they would not go beyond old-fashioned ways of investigations is unavoidable, in order to prevent nefarious activities [3]. As previously mentioned, their operation resides in identifying perpetrators, analyzing evidence and introducing solutions for existent problems. Leading agencies are burdened with the responsibility of continuously training their personnel and communicating with the public. Let us not forget that, as technology has rapidly developed through the past years, the public does not possess even the slightest knowledge about Internet issues; or they are even afraid of it. Thus, it can be easily concluded that CCUs perform another great task. They are obliged to inform common people, in plain terms, for the potential dangers behind the Internet and council them accordingly, to successfully prevent cybercrime. This kind of interaction with the public is called *engagement* and will be examined in the following chapters.

# 2 Social Media Platforms and Users' Data

## 2.1 Data Storage from Social Media Platforms

As described in Chapter 1, SMPs collect a wide range of data from their users. This information is usually obtained through the registration phase, which is mandatory for everyone, in order to create his/her uniquely identified profile. To add things up, every developing team related to a SMP's activities, was obligated to collect, and manage a chaotic amount of data, which is being shared by the users through their provided content. Hence, operators had to adopt suitable mechanisms to ensure that the users' data are being well organized and structured. In addition to all these technical issues, they had to reassure their users that their information is constantly secure.

Even though data storing policies posed as a simple requirement for most SMP companies, they became quite challenging in the process. The main reasons behind the faced difficulties were two. Firstly, the growing concerns from users regarding the mining of their personal data. Secondly, the colossal amount of processed information. What is dubious about data storage from SMPs, is the doubts that every "cybernaut" poses while using them. *"For how long is my personal information stored? What happens in the case of a data breach? Who will protect my privacy from a possible hacking attack? Apart from social media companies, which other entity manipulates my personal data?".* SMPs' storage policies were only restricted by the Directive 95/46/EC. By combining the year that the Directive was legislated (1995) and the introduction date of Web 2.0. (2005), it is straightforwardly concluded that SMPs pretty much established their own storage and processing rules. This phenomenon, among others, gradually directed the European Union (EU) in legislating the General Data Protection Regulation (GDPR), in 2016, which led to a new era in the protection of users' personal data.

As SMPs increased their fame amongst the public, companies that own them faced unique constraints regarding data storage and processing latency. As depicted in **Figure 9**, the amount of generated data is beyond reach. The upcoming challenges were related to pilling up enormous amounts of data, immediate access to databases, and a continuously increased scale of data, accompanied with the necessity for flawless service in respect to the guaranteed aspect of reliability [29]. As a result, each company implemented some existing databases, while others deployed their development teams to create their own. It is very interesting to briefly discuss the different types of storage systems and architectures, as it has challenged the limits of many SMPs.

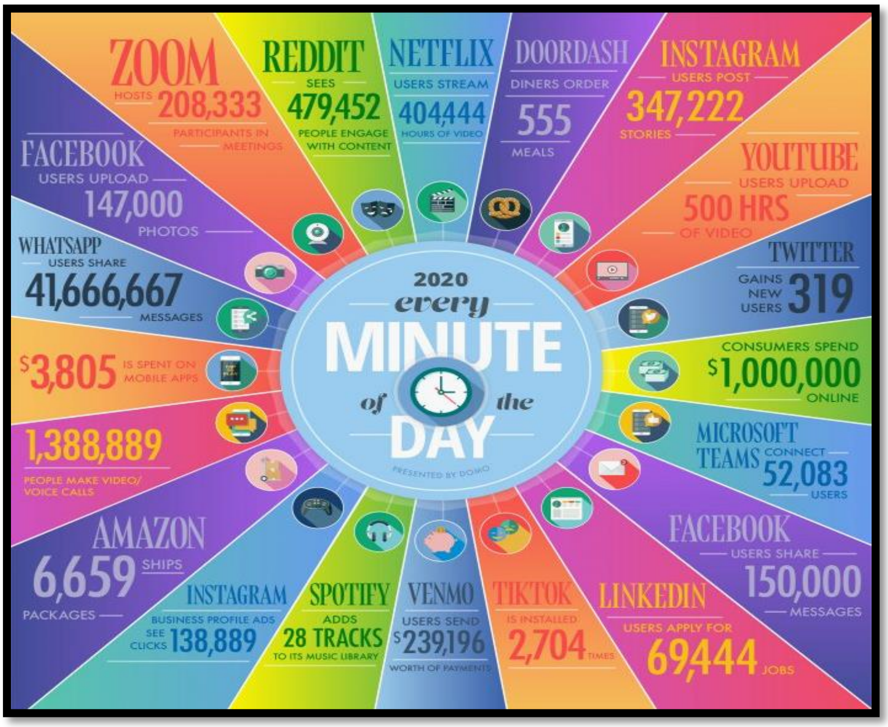


***Figure 9** : Data Never Sleeps 8.0*

### 2.1.1 BIG DATA

"Big Data" is a comparatively new-found term that describes the *"large set of data that is almost impossible to manage and process using traditional business intelligence tools."* [30]. This definition is usually being applied to, in two different situations. Firstly, concerning the challenges of storing and processing enormous amounts of data. Secondly, the term responds to the "sociological problem" formed by the realization that SNSs, or any other linked entities, methodically process and collect data involving their users [31].

"Big Data" has grown to be a major concern among SMPs. While user-generated data are growing immensely in number daily, human operators are no longer able to manipulate them. In specific, datasets regarding users' uploaded data are becoming unmanageable. One can easily come to the conclusion that any task that has to be performed on a controllable set of data, should be considered unfeasible when the number of imported data is unreachable. In other terms, an average user, who manipulates an insignificant amount of data for personal reasons (e.g., educational), can sufficiently manage them by using his/her personal computer (PC). Medium size data would require a different approach, such as parallel computing, in order to accomplish the desired outcome. Lastly, “Big Data” processing, demands more advanced means of performing, usually containing a substantial quantity of PCs with high-performing computer attributes, running specialized software and tools (e.g., MapReduce). The latter situation is what constitutes a “Big Data system” [32].

The term was originally conceived by Roger Mougalas, the market search director at O’Reily Media, in 2005. The fact that the organization coined another new definition, after the creation of the term “Web 2.0” a year earlier is quite remarkable [33]. Lots of studies and articles have been written concerning the effects of “Big Data” in the modern “Information Era”. Nowadays, an analysis of the term seems unavoidable. As “Big Data” definition proclaims, the amount of data has been so excessive that they demand more and more innovative means of processing.

The characteristics of “Big Data” are also known as the three “Vs”. To elucidate them, they are *Volume, Velocity* and *Variety*. These terms are used both to simplify the types of data and the software entities, which should be more suitable in manipulating them [34].

The *Volume* aspect constitutes the greatest challenge for computer engineers. They are presented the task of creating innovative structures, depending on scalable storage mechanisms and immediate acquisition of data. In plain terms, the Volume characteristic represents the nebulous amount of data produced, which is disproportionate with the amount of data that the traditionally used databases can afford.

*Velocity* describes the increased ratio of data, newly imported or exported by an organization. Albeit SMPs guarantee many services to their users, the key component is considered to be the constant and uninterrupted flow of data. As previously mentioned, many SMPs’ vital feature is the sharing of users’ content. Thus, it is important for users’ data to flow in a much higher speed, both imported into the company’s systems and exported to another user’s interface.

The final, widely accepted characteristic of “Big Data”, is *Variety*. It depicts the vast variety of data, which cannot be organized into correlated structures. For example, users’ presented information fluctuates, from photos and videos to texts. To make things messier, it can be easily understood that as far as computer communication is considered, exchanged data may rely on different kind of software, encoding, etc. This is a perfect example of how tricky the processing of “Big Data” can be [33].

Technological systems and associated tools involved into processing of “Big Data” are [35]:

- *NoSQL databases*, which are a type of database that provides the means for storing and regaining data. “MongoDB”, “Apache CouchDB”, “Apache Cassandra”, “Apache HBase”, “Hypertable” and “Apache ZooKeeper” are some of the highly used NoSQL DBs for “Big Data”.
- *MapReduce***,** which stands for the programming algorithms that process the data. The most famous MapReduce system is the “Apache Hadoop”. Other known systems are the “Apache Hive”, the “Apache Pig” and “Cascading”.
- *Storage services*, like “S3” and the “Hadoop Distribute File System” (HDFS).
- *Servers*, such as “EC2”, “Google App Engine”, “Elastic Beanstalk” and “Herokou”.
- *Processing tools*. Most known are the “R project”, “Yahoo! Pipes”, “Amazon Mechanical Turk”, “Elastic Search”, “BigSheets” and “Tinkerpop”.
- *Natural language processing (NLP).* NLP’s significance is embedded in the fact that they were created in order to process and comprehend unmeaningful humanly provided data. The component contains a variety of tools like “Apache OpenNLP”, “Boilerpipe”, “OpenCalais” and “Natural Language Toolkit” (NLTK).
- *Machine Learning systems,* with most commonly known services, the “Apache MAHOUT” and the “WEKA” frameworks.
- The graphical representation of data, which is called *Visualization.* Namely, tools involved are “Gephi”, “GraphViz”, “Processing”, “Tableau” and “Fusion Tables”.
- *Acquisition***,** for working with so-called “messy data”, as “Google Refine”.

The phenomenon of “Big Data” has created a lot of issues regarding users’ data privacy. Whilst a single user may generously upload his/her personal data, supposing that they are considered to be his/her own “property”, the overall percentage of imported data may easily create many confidentiality implications, due to insufficient protection [36]. Uploaded content, such as images, may contain information regarding another user, without him/her being aware of the situation. In more technical terms, a file’s metadata usually contains information regarding locations, time, etc., which may not only affect the owner of the file, but others as well. Related to this problem, resides the reference to a person who may have no association with the content itself. For instance, a photo containing a (hyper-) link or a “textual reference”, indicating another user’s profile, may cause serious harm to his/her personal data [31].

Last but not least, it is common sense that as SMPs constitute a modernized means of communication and information, there are users who will try to take advantage of their consistency and provide, either intentionally or unintentionally, fake information [37]. Malicious users tend to spread different kinds of fake information, causing all sorts of reactions, usually intending to create mayhem or to gain personal profit (fraud-related cases). In addition, unsuspected users tend to share the misleading information, with no regard to the outcome of their actions. A very vivid example related to present situations could be the wide spread of conspiracy theories regarding coronavirus. Although there are no countermeasures in order to avoid these problems, awareness is the key to eradicate them.

### 2.1.2 Databases, architectures, and storage systems

Every SMP embraces its own storage techniques, in order to process, store or manipulate in any way the imported data. Mainly, SMPs use Distributed Storage Systems (DSS) [38]. DSSs provide storage techniques, with which users’ data are partitioned, meaning that data are being split into different servers. This component provides high availability of data, even in cases of retrieving failure [39]. Deployed storage systems’ techniques and architectures could easily be a thesis’ main theme, therefore, only a brief description of them will be given in this chapter.

“MySQL” is considered to be the most stable and reliable database for storing data. With this database, the storage of data is performed once, whilst in others, data entries are stored twice or even more. Creating and installing this DB is quite simple, thus it is usually preferred by developers.

“Redis” and “Riak” are “key-value” storage systems, denoting that the mechanism of storing imported data involves creating keys that refer to the stored values. The difference between these two DBs is that while “Redis” supports lists of all ids-keys, “Riak” supports JSON documents, which is a great feature for storing SMPs’ “Big Data”.

“MongoDB” and “CouchDB” are the document storage databases, which use the same data model. They also support JSON or BSON files, similarly to “Riak”. The fact that these two DBs provide availability for storing any kind of data, is quite remarkable.

"Hbase" and "Cassandra", store the data in columns and depict them in a semi-structured manned, analogous to the document stores and "Riak". They provide the combining of both document and key-value store [40].

To conclude the enumeration of DBs, "Neo4j" is a "graph database", meaning that data are stored in graphical structure. With "Neo4j", SMPs do not only store users' data. Instead, they create "data relationships", indicating that they can visualize data within their native origin [41].

The most well-known storage system, used by SMPs, is called "Cassandra" and it is a NoSQL database management system. It was originally deployed for "Facebook", to empower its inbox search feature. Nowadays, it is used as an Apache Project by most SMPs like "Twitter" and "Reddit". The fact that it provides top level write processes, without losing read effectiveness is highly important in "Cassandra" technologies. In "Cassandra", the data storage techniques are based upon continuous "hashing" of the values, meaning that data is "hashed" to various data storage servers [39]. As defined, a "hash value" is *"a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures"* [42].

"Twitter" is one of the most prominent SNSs. Millions of users' "tweet" their stories and opinions every day. As the amount of imported data is chaotic, the company's founders had to adopt the appropriate infrastructure. "Twitter" had experimented with many databases over the years and made several contributions to them. But, on most occasions the developers understood that the deployed storage systems could simply not sustain the various products and services offered by the SNS. Consequently, they decided to build by themselves the next-generation DSS, called "Mahnattan" [29]. As depicted in **Figure 10**, "Manhattan" [43] and "Hadoop" [44] are the dominant systems (data-platform and database) used in "Twitter's" technologies.

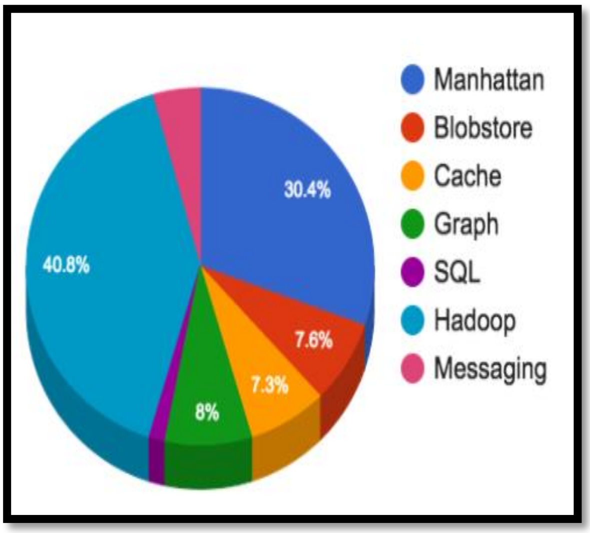


***Figure 10****: Services provided by Twitter's storage and messaging teams*

“Facebook”, which is the most famous SNS in 2020, with over 2 billion users widely, relied on relational “MySQL” DB for data storage [45], in addition to a variety of different engines. “Facebook” uses the “social graph” in order to record all users’ activity through its virtual society. A very common example is the tracking of who “liked” another user’s uploaded content. This “social graph” is empowered by “MySQL”. Moreover, Facebook Messaging was originally stored in “Hbase” [46], whilst nowadays the component uses “MyRocks”, which integrates “RocksDB” and “MySQL” storage engines [47]. Other used databases are “Apache Hadoop”, “Apache Thrift” and “PrestoDB” for manipulation of “Big Data”, and “LogDevice”, as a storage system for users’ log data [48].

Even though “Google LLC” is not a company that provides social networking services, it is one of the largest companies worldwide, numbering many applications that could be easily considered as SMPs (e.g., “YouTube”). “Google LLC” has established its private “Data Centers” to store and process the nebulous amount of information, of its million users. In these centers, the company runs its services 24/7. They consist of aisles of server racks (“Google Web Servers”), which run the distributed data storage systems (“Big Table” [49]) and the scale-databases (“Spanner”). Needless to mention that these technologies were created and founded by the company’s technical team [50].

Finally, it is critical to enumerate some of the architectures related to “Big Data” storage technologies. Mainly they involve [31]:

- *Multiple clustered network attached storage (NAS).* NAS is a computer data storage server, connected to a network. Clustered NAS, is a NAS which uses different storage devices inside a network, using a single file system which is running simultaneously. Multiple clustered NAS is the system in which clustered NASs form different networks are employed together.
- *Object-based storage techniques, like Hadoop distributed file system (HDFS).* In this scheme, the employed storage system manipulates unstructured or semi structured data. Hadoop is a data storage system, created to process a vast volume of data.
- *NoSql databases, MoonDB* and *Terra Store* are used to manipulate structured data.
- *Apache Avro* conceived in terms of nodes communication,
- *Cassandra* and *Hbase* designed to work with Hadoop.
- *Hive,* a system like SQL, but working with Hadoop.

- *Mahoot*, a tool created for machine learning.
- *Pig Latin* and *Zookeeper*.

### 2.1.3 What types of Data?

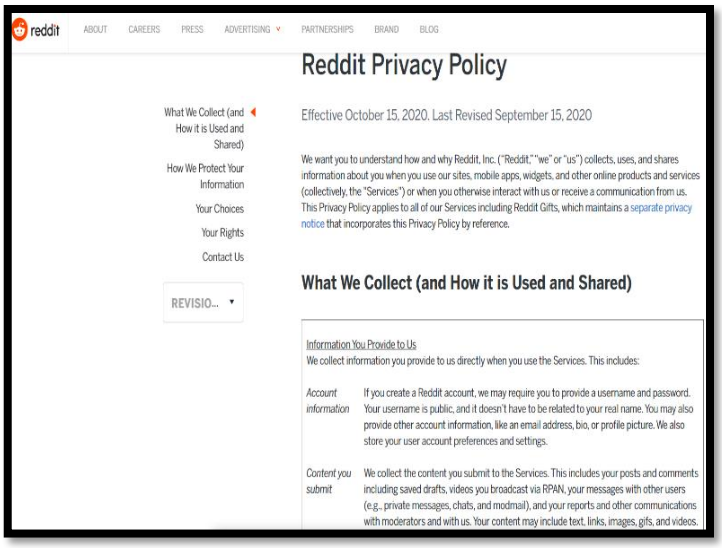
Up to this point, this Chapter has deepened into the challenges that SMPs face regarding processing users' data, as well as the deployed storage mechanisms which assist in curtailing them. Thus, a presentation of what types of data each SMP stores or processes is deemed necessary.

"Facebook" collects all sorts of information regarding its users and their content. The company's systems automatically process data related to *the content itself, date and time* of creation or sharing, and *metadata*, such as the location of a photo. Moreover, the user may choose to provide certain types of *"sensitive personal data" (see below, p. 28)*, within his/her profile, such as *religious* or *political views*, *health statuses*, *racial or ethnic origin*. To add things up, the SMP stores *network and connectivity information***,** most importantly *IP addresses*, *name of ISP*, *time zone*, *mobile phone number*, and as stated in "Facebook's" privacy page, *"in some cases, information about other devices that are nearby or on your network"*. Lastly, the automated systems process data related to *device information, usage and transactions regarding "Facebook's" products, information from partners or affiliated parties and cookies data* [51]**.**

According to "Twitter's" privacy policy, the company processes data regarding basic information like *provided e-mail or phone number*, users' preferred *time-zone and language, date and time* of uploaded content. As far as messaging is concerned, "Twitter" stores and processes data regarding enhanced *images, links or unified resource locators (URLs)* and the *communication information* (sender-receiver and data). The fact that the company does not store the content of the messages is remarkable. Additionally, *location, cookies, payment and log data (IP addresses, web browser, operating system, etc.) information* are also stored by the SNS's systems [52].

"Tinder", which is the leading dating application in 2020, also collects a substantial variety of data. *Login credential (username and password)* and basic information, like *gender* or *age*, are data stored during the registration phase. Once an account is created, the SNS requests and processes details of a user's *personality, lifestyle or interests* and content like *photos or videos*. This information is requested to fix up the users' profile and it also is a prerequisite in the match-making procedure. The company also stores *messaging content, payment information, associated or verified social media accounts and information that other users provide* them with. Finally, the SMP processes *device, networking, geolocation* information and most importantly, *the way that a user interacts/connects with another user* (accounts, number of messages, etc.) [53].

As mentioned in Chapter 1, another major part of SMPs are “content communities”. “Reddit” is one of the most prominent ones, used by millions of clients. As any other SMP, “Reddit” has its own privacy policy, as demonstrated in **Figure 11**. In this privacy policy”, the company explains in plain terms, the procedure regarding processing users’ data. According to it, the “content-community” platform, separates the collected data in three types. The information that the users provide on their own, the information that the platform’s systems process automatically and the data the company collects by other sources and third parties. The users’ provided information varies from *account* data and *content*, to *transactional* information and *interactions with other users* (e.g., blocking or following). Automatically collected information consists of *log* and *usage data*, *cookies*, and *geolocation*. In the end of the privacy policy, there is an additional field in which the designers emphasize that, apart from the previously mentioned information, the SMP also acquires data related to a user, from *third parties* (for example embedded content through “YouTube”), *other sources* (e.g., a third-party mobile application) and *advertisers* (reddit adds) [54].



Reddit Privacy Policy

Effective October 15, 2020. Last Revised September 15, 2020

We want you to understand how and why Reddit, Inc. (“Reddit,” “we” or “us”) collects, uses, and shares information about you when you use our sites, mobile apps, widgets, and other online products and services (collectively, the “Services”) or when you otherwise interact with us or receive a communication from us. This Privacy Policy applies to all of our Services including Reddit Gifts, which maintains a separate privacy notice that incorporates this Privacy Policy by reference.

What We Collect (and How it is Used and Shared)

Information You Provide to Us
We collect information you provide to us directly when you use the Services. This includes:

*Account information* If you create a Reddit account, we may require you to provide a username and password. Your username is public, and it doesn’t have to be related to your real name. You may also provide other account information, like an email address, bio, or profile picture. We also store your user account preferences and settings.

*Content you submit* We collect the content you submit to the Services. This includes your posts and comments including saved drafts, videos you broadcast via RPAN, your messages with other users (e.g., private messages, chats, and modmail), and your reports and other communications with moderators and with us. Your content may include text, links, images, gifs, and videos.

***Figure 11****: Reddit Privacy Policy*

From what has been analyzed so far, one can easily conclude that every SMP stores and processes, in great extent, the same type of users’ information. There might be some divergences from one platform to another, nonetheless the essential acquired data are the same: e-mails and passwords (as registration data), content, location and networking information. Nowadays, all SMPs thoroughly describe the kind of processed data to their potential “cybernauts”, through their integrated privacy policies. They deliberately request users’ consent to process their data, as it is mandatory due to the GDPR. But was this explicit consent always compulsory for social media companies?

## 2.2 Law Change – GDPR

Privacy and data protection are two rights enshrined in the EU Treaties and in the EU Charter of Fundamental Rights. The Charter contains an explicit right to the protection of personal data (Article 8). The Charter of Fundamental Rights has the same legal value as the constitutional treaties of the EU. In addition, Article 16 of the Treaty on the Functioning of the European Union (TFEU) obliges the EU to lay down data protection rules for the processing of personal data. The EU is unique in implementing such an obligation to its constitution.

The GDPR came into effect in 2018 and constitutes a modern framework for Data Protection in Europe. The European Parliament voted for it in May 2016. Up to that point, data protection in the EU was mainly regulated by the Data Protection Directive 95/46/EC. Moreover, the European Convention for the Protection of Human Rights and Fundamental Freedoms (referred to as the European Convention on Human Rights – ECHR) was drafted by the Council of Europe in 1950 and entered into force in 1953 (Council of Europe, 1950). In Article 8 of the ECHR, (*“Right to respect for private and family life”*), is specifically provided that *“Everyone has the right to respect for his private and family life, his home and his correspondence.”*.

Since the Directive was legislated in 1995, it is particularly apparent that due to the major blossom of SMPs around 2005, which adopted numerous automated systems for processing personal data, a new legislation safeguarding “netizens’” personal information was of outmost necessity [55]. Even though the Directive formed the first EU legislation regarding data protection and widely defined the various forms of information, the GDPR remodeled its provisions and principles, making it more appropriate for the new “Information Era”.

The main difference which makes GDPR more suitable nowadays can, in the view of the author, be restrained in two main facts. Firstly, the Regulation introduced many changes, compared to the repealed Directive, mainly related to the pragmatic application in all processing entities and their territorial scope. Secondly, it generated much more practical implications to the technical design and privacy protection measures of “data controllers and data processors”, regarding data storage, processing and implementations of security practices.

### 2.2.1 Brief presentation of the GDPR

The GDPR is the EU regulation under number (EU) 2016/679 (General Data Protection Regulation) and it came into effect on the 25th of May 2018. In general terms, it provides a detailed framework in which processing entities learn how to process, inform, and secure “data subjects’” personal information.

The GDPR is a legal instrument, consisting of 99 Articles. It is a “Regulation”, meaning that this legal text is binding and applies directly to all EU’s members. In Greece, the Parliament adopted Law 4624/2019, implementing the GDPR and transposing into national Law, the Law Enforcement Directive 2016/680 (LED). Law 4624/2019 abolishes, with a few exceptions, former data protection legislation, namely Law 2472/1997.

But what is Data Protection? According to Article 8 paragraph 1 of the EU Charter of Fundamental Rights: *“Everyone has the right to the protection of personal data concerning him or her.”* Taking into consideration this Article, every person has the right to access or delete his/her digital content and to be notified about whether information that refers to him/her as an individual, is being processed in any way. Hence, any entity that handles a subject’s information is obliged to perform these activities based on the individual’s consent or any other legitimate basis. In Article 6 of the GDPR there is a detailed list which fully explains the grounds upon the processing of data is founded on a legitimate basis.

The categories of data that the GDPR aims to protect are the so called “personal data” as defined in Article 4(1) GDPR. According to the provided definition, *“‘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.”*. “Personal Data” are the following, for example:

1. Personal information that uniquely identify a person (e.g. name),
2. Communication Data,
3. Sexual orientations,

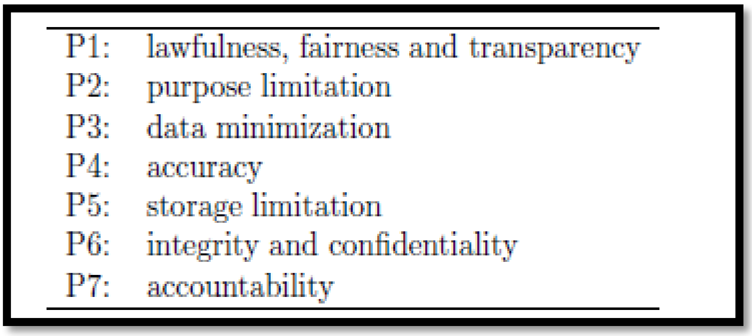
4. Political opinions,
5. Religious or philosophical beliefs,
6. Health and genetic data,
7. Racial and/or ethnic data, and
8. Biometric data.

Some of the above-mentioned information is considered *"sensitive"* and it alludes to an individual's *sexual, political, religious, health* and *racial* information. In general terms, "sensitive data" are information that ought to be prioritized in cases of security breaches. Unauthorized access to this kind of information is forbidden (Article 9(1) GDPR). Exposure of "sensitive data" is strictly undesirable [56]. The protection of this information is required due to ethical reasons or concerns related to an individual's privacy. Therefore, the EU put into force solid regulations and severe penalties concerning personal "sensitive data".

Any entity that stores or processes personal data of a given subject is obliged to be compliant with the GDPR. A *"data subject"* is the identified or identifiable natural person to whom the data relate (Article 4(1) GDPR). A *"data controller"* is the natural or legal person, public authority, Agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (Article 4(7) GDPR). Finally, a *"data processor"* is a natural or legal person, public authority, Agency, or any other body which processes personal data on behalf of the controller (Article 4(8) GDPR).

The Regulation provides several preconditions, mostly territorial, in which an entity is subject to the GDPR. According to Article 3 of the GDPR, the territorial scope of the Regulation has been extended and it applies to all EU-based controllers and processors, irrespective to the physical location of data processing. Additionally, the GDPR applies to all entities, which offer services or material goods to a "data subject" in the EU. Finally, the territorial appliance of the Regulation extends to entities that monitor data subjects' behavior within the EU [57].

According to the GDPR, the introduction of new terms, definitions and principles is new as well. These definitions are primarily linked to processing companies and their related activities. In particular, the Regulation has included new terms and principles concerning processing like: *"transparency"* and *"accountability"* (Article 5) and *"Processing which* *does not require identification."* (Article 11). Moreover, it has implemented new definitions such as: *"pseudonymization", "data protection policies" and "data breach"*. The fundamental principles of the Regulation are seven (7) and they are the ones depicted in **Figure 12** [58]. Ultimately, the most significant impact of the Regulation, is the induction of countermeasures against unlawful and irrational data processing. These countermeasures are described in the embedded Articles describing the rights of data subjects and penalties for entities who fail to comply [59].



| | |
|---|---|
| P1: | lawfulness, fairness and transparency |
| P2: | purpose limitation |
| P3: | data minimization |
| P4: | accuracy |
| P5: | storage limitation |
| P6: | integrity and confidentiality |
| P7: | accountability |

***Figure 12****: The seven basic principles in the GDPR*

For data to be processed lawfully, the processing must comply with one of the lawful grounds for making data processing legitimate, listed in Article 6 GDPR for non-sensitive personal data, and in Article 9 GDPR for special categories of data (or sensitive data).

Last but not least, it is of outmost necessity to mention, once more, that whenever a company processes information in an unlawful way, it might be held accountable for it and be fined for its violations. These violations can be due to an action or a negligence of the entity in question. According to Articles 58 and 83 of the GDPR, the competent supervisory authority of a member state (in Greece it is called "Hellenic Data Protection Authority") has the power to investigate and to fine any entity which does not abide by the legal provisions.

Moreover, the GDPR has introduced a not so new concept for the purpose of handling data protection issues. This concept is known as the "Data Protection Officer" (DPO). "Data Protection Officers" are persons who advise on compliance with data protection rules in organizations undertaking data processing. They are considered 'a cornerstone of accountability' because they facilitate compliance. Furthermore, they function as intermediaries between the supervisory authorities, data subjects and the organizations that appointed them.

Taking into consideration all the facts mentioned above, one may conclude that the GDPR is a Regulation formed to protect individuals' rights. As we live in an era in which everything is digitalized, it is essential for all entities to understand the importance of data protection and make their best efforts to ensure that no violations occur. As SMPs are essentially the major data generators in our "Information Era", they are responsible for adopting the Regulation's methods of protection and be compliant to it.

It must be noted that the GDPR excludes from its scope data processing by competent authorities for 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 (Art. 2(2)(d) GDPR) and paves the way for the so-called Law Enforcement Directive (LED), which applies to data processing 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.

### 2.2.2 Data Protection through GDPR – Users' Rights

Since the popularity of SMPs has grown immensely over the past few years, like "Facebook" or "Pinterest", they are considered to be the online communication's key mediators. Even though users are provided with many benefits, privacy related concerns have increased. The excessive use of SMPs has gradually led to the phenomenon of users losing control over their personal data, to the point that an individual's provided content is no longer considered as his/her private property [60]. To ensure that data controllers no longer make unnecessary processing of users' data, the GDPR provides "netizens" with several protecting rights. All in all, these rights aim at giving individuals full control of the data related, in any possible way, to them.

According to Article 12 of the Regulation, data processors and controllers are obliged to inform data subjects, at the time when personal data are collected about their intended processing. Plainly, GDPR compels entities to thoroughly inform the data subjects concerning their personal data processing and to provide this information in a *"transparent, intelligible and easily accessible form, using clear and plain language"*. Additionally, Articles 13 and 14 enlist the information that must be provided by the entities in question. These Articles represent a data subject's *"right to be informed"*.

Moreover, Article 15 has introduced the right of a data subject to access his/her personal information, processed by the data controller. Specifically, a user may inquire whether his/her personal information is being processed and in case s/he gets an affirmative response, s/he has the right to access it, request and receive a copy *"in a commonly used electronic form"* and acquire any other additional information (reasons for processing, etc.). The period for providing the requested information is set to one month (Article 12(3) GDPR). As the title proclaims, Article 15 establishes *"the right to access"*.

Articles 16 and 17 provide to data subjects' the rights to *"rectification"* and *"data erasure"* respectively. The "right to rectification" enables data subjects to request inaccurate, incorrect or incomplete information to be altered, in his/her desired way [61]. Conversely, with the "right for erasure", the GDPR provides the conditions under which a data subject may obtain the deletion of his/her private information and refraining data processors/controllers from additional distribution. The "right of erasure" is based on the *"right to be forgotten principle"* and its prerequisites consist of: (i) unnecessity of data processing, in relation to the original purposes, (ii) withdrawal of data subject's consent, (iii) data subject's objection to processing, (iv) unlawful process, (v) a legal obligation which demands the erasure of processed personal data and (vi) data were processed for the purpose of offering information society services to a child. Clearly, since many times requests for data erasure may exceed the purpose of the Regulation, the legislators have put into force several occasions in which organizations may deny erasing personal data.

Furthermore, under the Regulation, restriction of processing should be considered sufficient in some cases, instead of erasing the data. The *"right to restriction of personal data"* proposes an alternate to data erasure and it is performed in several instances, explicitly mentioned in Article 18 GDPR. Generally, *data restriction* is obtained in cases of unlawful processing, objection of processing by the data subject, acquisition of information by data subject for legal reasons and pending challenging of inaccurate data. In any event, according to Article 19 GDPR, the entity is obliged to inform the data subject before lifting the ongoing restriction.

A new right provided by the Regulation is that of *"data portability"* (Article 20 GDPR). According to this right, data subjects are entitled to acquire data which have been provided to a controller (either by consent or contract), for automated processing. Also, the user may ask for these data to be directly transmitted from one entity to another. Surely, the exercise of this right has once again some restrictions, mostly involving affecting rights and freedoms of others or distorting the *"right to be forgotten"*.

Articles 21 and 22 provide the rights to a data subject, to *"object data processing"* and *"not to be subject to automated individual decisions*". The first Article provides the right to object, meaning that a data subject may deny data processing for certain specified purposes, in occasions related to his/her individual conditions. Article 22 provides restrictions regarding a user being subject to a decision-making, exclusively by automated processing of his/her data. In any case, Article 22 refers to situations where the automated processing is intended for evaluating the data subject's personal aspects [62].

In conclusion, the GDPR offers a wide range of protective measures to data subjects. As far as data processing and security are concerned, the legislators have introduced several obligations for the entities which are engaged in these forms of activities. The Regulation mandates that data controllers/processors are obliged to adopt the appropriate techniques and mechanisms which secure data subjects' data and provide a legitimate data processing in general. In addition, a supervisory authority is to be established in every member state, which constitutes the institution that supervises and collaborates with all data controllers/processors, within the states' territory. As already mentioned, the GDPR has also introduced a new role, that of the DPO, who is an organization's advisor regarding data protection. Lastly, Articles 77-84 of the Regulation offer the ability to a data subject to lodge complaints and compel supervising authorities to take actions and fine entities, in cases of verified infringements of data protection.

## 2.3 Social Media and GDPR

Given the challenges of Web 2.0., the member states of the EU acknowledged the fact that the Data Protection Directive 95/46/EC was obsolete and could not guard users sufficiently anymore. GDPR's being put into force required many updates regarding other EU regulations, and it was a procedure that kickstarted in 2012 [55]. With the enactment of the Regulation, natural persons were protected from unauthorized and unlawful processing of their data. Still, the enactment of a legal text does not mean that privacy dilemmas disappear in a magical way.

In subsections 2.1.1 and 2.1.2, the reasons behind implementation of improved storage techniques and databases have been analyzed. The vast amount of imported data led to the deployment of those mechanisms, which on many occasions are performed automatically. Since humans were simply not capable of handling the processed information, machines were brought into action. However, it is obvious that the software, the servers, and the data acquisition systems are handled by humans. Nobody should have the privilege, or on some occasions carry the burden, of having unlimited access to an individual's private information. Therefore, controllers/processors had to alter their policies and be consistent with the Regulation. As SMPs constitute the content generator industry, by constructing enormous online communities, they were the first entities responsible for abiding by the new rules and conform with the GDPR.

### 2.3.1 Implementation of new Policies

Internet companies have had enough time to realize that they should use safeguards in data collection. Limiting the storage of unwanted data and adopting international security standards should be their foremost concern. On the contrary, data misuse incidents were more than often, including data security breaches or unlawful transportation of data to unreliable third parties. One of the most impactful data breaches was that of "Yahoo!" in 2014, where approximately 500 million user accounts were stolen [63]. Another major data breach was the one occurred in "LinkedIn's" network in 2012, during which a Russian hacker named "Peace" exploited the SMP's systems and sold the compromised data on a dark web marketplace [64]. Conclusively, these incidents led to the fact that as online communities expanded, users gradually lost control over their own data. Thus, by legislating the GDPR, EU targeted at providing "cybernauts" with extensive control over their private information.

*"Pseudonymization"* and *"encryption"* are the two key-factors that can potentially guarantee SMPs' protection of users' data. Albeit, these terms seem quite familiar in a computer science community, implementation in such a vast data generator company, requires state of the art techniques and efficient data storage mechanisms. *"Pseudonymization"* is a widely known de-identification procedure, implanted by the GDPR, and is defined both as a data protection mechanism and a security measure, against unlawful access. Well known *"pseudonymization"* techniques are *hashing, random number generator (RNG), tokenization,* etc. [65].

*"Encryption"* of data is a technique of achieving *"pseudonymization"*. In computers' science sphere, *"encryption"* of data is defined as the conversion of data from a readable

format to an encoded cipher. There are several methods applied in encoding and decoding data, mostly involving *"Symmetric key cryptography"* and *"Asymmetric cryptography"* [66]. Encrypting users' data in SMPs is quite challenging, due to the "Big Data" theorem. Indeed, SMPs' engineers have either created or applied the appropriate *"encryption"* schemes, as GDPR obligates them to do so. For instance, "Facebook" had originally selected "Kerberos" system to encrypt users' data, but in order to balance security and operability of systems, the company implemented "Transport Layer Security" (TLS) [67].

Along with all other changes, SMPs had to alter their privacy policies. As defined by the Australian government: *"A privacy policy is a statement that explains in simple language how an organization or agency handles a person's personal information."* [68]. Therefore, as SMPs handle users' personal data extensively, they were obliged to inform them about the reasons and the proceedings of data processing. Implementation of a privacy policy is the solution to the principle of *"transparency"*, provided by the GDPR, and designates the first step that makes a SMP compliant to the Regulation.

Privacy policy texts, created by SMPs are often overlooked, as they are too extensive or simply too boring for the average user. In fact, "Twitter's" privacy policy is nineteen pages long [52], "Tumblr's" is eight pages long [69], and so on. If in doubt, you can simply ask yourself, *"Have I ever read a privacy policy document, or just clicked on the accept button?".*

Although privacy policies should be easily comprehended by a user, they must cover the entire spectrum related to data processing. A standardized privacy policy text created and provided by a SMP, should contain explicit information corresponding to the following questions [70]:

1. Who collects the personal data?
2. Who uses the collected data?
3. Which data are being processed?
4. How long is the retention period?
5. What is the reason for data processing?
6. How can a user exercise his/her rights?
7. What are the securities measures?
8. Is the user notified when a change to privacy policy occurs?

Provided that a privacy policy document answers these questions, it should be considered as GDPR compliant.

Even though, GDPR has come into force in 2018, there are still many entities which fail to comply. Some companies have not implemented well informed privacy policies, whilst others do not support mechanisms that respond to users' queries. The main focus of SMPs should be strictly limited on providing users full control of their data. Along with a fully structured privacy policy, SMPs must deploy storage mechanisms that automatically erase data from all internal systems (after a certain retention period). Also, they must support techniques which allow data subjects to immediately access the processed data and be easily provided with a copy of them (easily handled requesting platforms and readable provided formats). Finally, as limited access and privacy of data are of outmost necessity, each SMP must adopt the appropriate encryption and access techniques that are suitable for its implemented storage systems [70].

# 3 Social Media Platforms and Law Enforcement

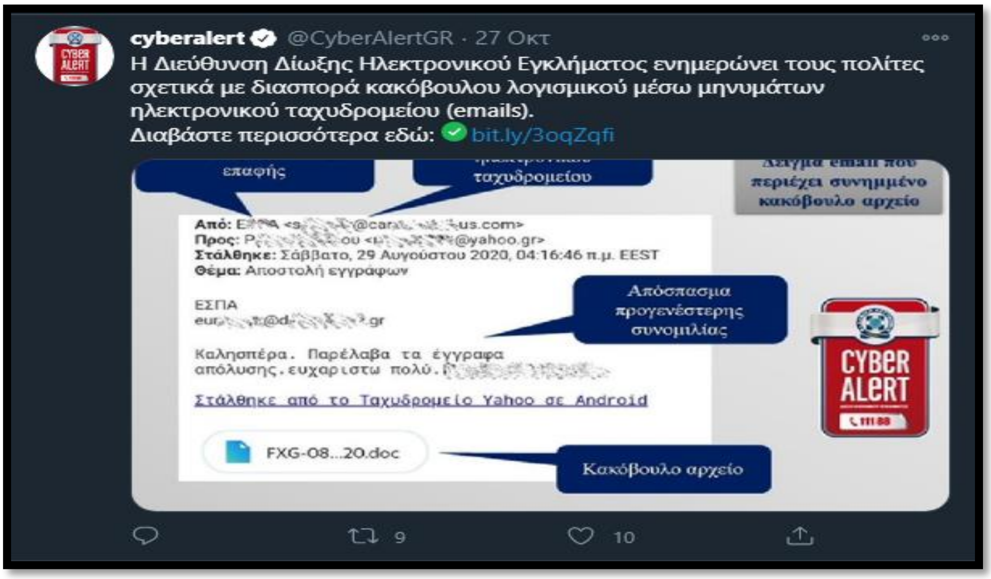
Social Media Platforms provide a variety of advantages to the public. Cybernetic communities comprise a welcoming environment for all people. No-one is banned from registering; as long as users comply to a SMP's terms of services, they can keep their uniquely identified profiles and enrich these societies with their distributed content. But beyond the majority of users who join a SMP to share knowledge, communicate with others, or enjoy its services in any possible way, there is a small percentage who will try to leverage its merits in order to gain unlawful profit. Lots of complaints have been lodged against users who have harassed or bullied others. Additionally, courts have tried several fraud-related lawsuits or to make things even worse, child sexual abuse/exploitation cases. It appears to be quite apparent that social media, and in specific SNSs, are potential goldmines for criminals. To deter these activities, SMPs have implemented quite a few reporting mechanisms in order to ban antisocial users. These mechanisms should be considered quite adequate when it comes to misdemeanors, like hateful speech or defamation. But what happens when a felony occurs? How do SMPs inform police authorities, for any impending criminal activities? And most importantly, how do law enforcers acquire the evidence of such a crime or the data of the cyber perpetrator [71].

Although in chapter 1 the definition of cybercrime and its general concepts have been provided, in this chapter this thesis will analyze the different types of cybercrime occurring in SMPs. Cybercrime is a specialized form of crime and it is fed by the dynamism of cybersphere [72]. For over two decades, traditional criminals have realized the importance of becoming active in cyberspace; but exploiting any system is not easy. Hacking is the field of computer science that requires both programming/networking knowledge and flair. Thus, criminals that do not share the passion for computing, had to come up with other means of breaking the law. Sometimes they achieve their purposes and sometimes they do not. As cyber criminals and their practices have progressed a lot through time, police agencies had to keep up with their evolution, in order to protect citizens' rights. Apart from upgrading their skills, training and equipment, law enforcers were obliged to form an alliance with the entities which were responsible for controlling almost every users' data, globally. What these entities do is witness the blossom of cybercrime and try to prevent it from occurring in its core. These entities are no others than Social Media Platforms.

LEAs could not afford being absent from social media. It was simply not an option. This new reality of events was not just an outcome of rapid reproduction of different types of cybercrime. Society's demands grew immensely, to the point that police's traditional investigating and intelligence techniques were condemned as old-fashioned. Citizens expect police to be always one step ahead of criminals. Informing the public or arresting lawbreakers are mandatory actions that provide the public with the feeling of security. People expect faster reactions and effective handling of crime-related situations [73]. Since criminals realized that cybercrime is the future of gaining unlawful profit, they have become technologically aware and left the police fighting with petty theft and misdemeanors. The use of SMPs can provide many benefits to all LEAs. Data acquisition, public interaction and innovative investigation techniques, are merely some of the modernized practices that bridged the gap between cybercriminals and the police.

Police agencies use SMPs in three main areas: *engagement, intelligence* and *enforcement* [74]. *Engagement* is the field which covers LEAs' interaction with the public. Nowadays, communication is the key to all aspects of life. Police needs this communication. Apart from informing society about their practices, they need to be engaged too. People's provided information could be vital in solving all sorts of incidents. Engagement via SMPs is very important, as it should provide police officers with the opportunity of influencing the public and widening their access to the community [75]. Moreover, an uploaded post in any SMP, can provide multiple safety related advice, concerning impending cybercrimes, inspire people to be aware of any criminal activity in their community and to propose methods in order to minimize the risks. A noted example is the "Twitter" account, set up by the Hellenic Cyber Crime Unit, as depicted in **Figure 13**, through which the Police Agency provides all sort of information to its followers, who can read and share it at the click of a button, spreading the news to a large number of people. All in all, engagement provides quick and effective communication between Police and the public.

*Intelligence* and *enforcement* are the two areas which will be thoroughly studied in this chapter. SMPs attract users from all walks of life and store their data in their systems. As priorly explained, the "Big Data" phenomenon has led to the creation of many concerns involving security and privacy of users' information. Nevertheless, if manipulated intelligently and elegantly, it can profoundly be considered as a significant tool in preventing and investigating cybercrime [76].



cyberalert @CyberAlertGR · 27 Οκτ

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους πολίτες σχετικά με διασπορά κακόβουλου λογισμικού μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails).
Διαβάστε περισσότερα εδώ: ✓ bit.ly/3oqZqfi

Από: Ε[redacted] <s[redacted]@car[redacted]us.com>
Προς: Ρ[redacted]ου <[redacted]@yahoo.gr>
Στάλθηκε: Σάββατο, 29 Αυγούστου 2020, 04:16:46 π.μ. EEST
Θέμα: Αποστολή εγγράφων

ΕΣΠΑ
eu[redacted]@d[redacted].gr

Καλησπέρα. Παρέλαβα τα έγγραφα
απόλυσης.ευχαριστω πολύ.[redacted]

Στάλθηκε από το Ταχυδρομείο Yahoo σε Android

FXG-08...20.doc

επαφής
ταχυδρομείου
Δείγμα email που περιέχει συνημμένο κακόβουλο αρχείο
Απόσπασμα προγενέστερης συνομιλίας
Κακόβουλο αρχείο
CYBER ALERT
11188
9
10

***Figure 13****: Hellenic CCU's Twitter Page, informing the public for the spread of malware via e-mail*

SMPs can assist any Police Agency in information gathering and *intelligence*, regardless if the Agency is involved in the cybercrime field or not. The networking platforms can assist in cases of locating people, who are either missing or intending to commit suicide, through the disclosure of geolocation data. Additionally, SMPs can be used by LEAs as a helpful tool to obtain information after the commitment of a crime. Viewing an uploaded video regarding a committed criminal activity on "YouTube", or the recognition of a perpetrator through his/her "Facebook" account are common practices. Lastly, as prevention of criminal behavior is of outmost necessity for all LEAs, policemen deploy SMPs in order to monitor criminal activity of the community they serve, by picking up leads and preparing for any potential incidents. In addition to these practices, CCUs regularly visit websites, known for propagating hate speech or used by registered sex offenders, in order to target vulnerable victims [77].

*Enforcement* through SMPs is the key data acquisition method for CCUs. Through the following sections, the requests sent by LEAs in order to obtain data regarding unknown offenders, will be presented. As priorly mentioned, cyberspace offers anonymity to its users. Criminals tend to exploit this anonymity and remain unidentified while acting harmfully. Whereas other police agencies collapse, CCUs affiliate with SMPs and obtain data which, if handled accurately, can lead to the identification of the unknown perpetrator. In addition, CCUs have either adopted or fashioned various investigative techniques, like “Open-Source Intelligence” (O.S.INT.), social digital forensics and social media profiling, to support their public services. Gradually, collected IP addresses, registered e-mail accounts, metadata and any other provided information from SMPs, along with the collaboration of national ISPs, can solve an investigation, which in any other occasion would be abandoned and filed as a “cold case” *(i.e., an unsolved criminal investigation, that has stopped being actively pursued because of a lack of evidence* [78]*).*

## 3.1 Types of cybercrime on SMPs

As the use of SMPs escalates on an exponential basis, cybercrime activities become more and more aggressive. Crimes against the confidentiality, integrity and availability of targeted systems occur constantly. In chapter 1, this thesis has provided a historical preview of cybercrime along with its general concepts. Now it is time to present the most common criminal activities, committed in the heart of virtual communities: Social Media Platforms.

### 3.1.1 Personal Data Breach – Identity Theft

Corresponding to FBI’s annual Internet Crime Report for 2019 [79], which derives from the records of IC3, *personal data breach* counted 38,218 victims, while *identity theft* counted 16,053 victims in the U.S.A. According to the report, *“Identify theft involves a perpetrator stealing another person’s personal identifying information, such as name or Social Security number, without permission to commit fraud.”* [79]. The commitment of *identity theft* does no longer require the criminal’s real-life interaction with his/her victim. SMPs and in particular SNSs, have provided unlimited resources for the occurrence of this criminal activity. Nowadays, as people post their personal data freely online (such as photographs, occupation, family status, addresses, etc.), they attract criminals’ attention who seek to forge official documents. The acquisition of these data, jointly with the use of technically specialized tools (e.g., reverse lookup), which are available on the Internet free-of-charge, may result in stealing a user’s identity.

In EC3’s 2020 annual report [80], the organization has defined *personal data breach (compromise)* as *“the ability of criminals to access individual user credentials or to access large databases with potentially valuable information.”*. After the legislation of the

GDPR, the act of compromising someone’s personal data is considered quite heinous. The regulation obliges companies to report these kinds of breaches, as the protection of EU’s citizens personal information is deemed extremely important [80]. A distinctive example of a data breach criminal activity is the incident that took place in “Twitter’s” network, in 2020, where a seventeen-year-old hacker breached the SNS’s infrastructure and compromised dozens of accounts, belonging to several high-profile users (politicians, celebrities, entrepreneurs, etc.). In the end, the hacker and his accomplices managed to steal over 118,000$ worth of bitcoins (BTC) and exposed the infrastructure vulnerabilities of the platform [81] [82].

### 3.1.2 Cyberterrorism – Cyberthreats

As SMPs are widely used for the commitment of any sort of traditional crime (theft, sexual abuse, identity theft, espionage, etc.), violators tend to take advantage of cyberspace, in order to convey their hate speech and threaten others. When it comes in defining and categorizing cyberterrorists, the motivations behind the reproduction of hate speech are irrelevant. Usually, these acts of hate are caused by moral, religious, political or any other related ideas. The term was originally coined by Barry Collin, in 1980, and it still of use nowadays, having different meanings, depending on the nation or field of science that describes it [83]. *Cyberterrorism* is defined, by the IC3’s annual report, as *“Violent acts intended to create fear that are perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants.”* [79]. This definition is closer to the term *cyberthreat*, where users from distinct background, tend to pose imminent threats to a group of people who do not share their point of views regarding religion, politics or even sports. *Cyberthreats* are typically made in order to generate hate speech, by people who hide behind their screens and try to avoid personal confrontation. Therefore, violators rarely deliver them in practice.

In contrast, *cyberterrorism* applied in SMPs, has a different connotation. It involves the cyberattack, executed to penetrate a specific target, from all connected internal or external networks, by a group of people who share the same motivations. SMPs and the establishment of virtual communities, have created the appropriate background for the blossom of *cyberterrorism*. The relative ease of access, accompanied with the low-cost provision of services, deliver  a suitable environment, through which terrorists can forward their violent extremism, beyond the borders of their countries [84].

The United Nations Office on Drugs and Crime (UNODC), in its report on online terrorism, has categorized the main areas of *cyberterrorism's* utilization of SMPs, and Internet in general [85]. These categories are:

1. *Propaganda*. Terrorists recruit SMPs to spread their message and make the public sympathize with them. They try to justify their cause, by uploading videos, presentations, virtual messages, etc., through which they dare to enforce their perspective and recruit followers globally.
2. *Financing.* Another use of SMPs is the raise of funds to finance the acts of terrorism. Generally, terrorists ask for donations from SMPs' users, through direct messaging, advertisements, or any other available service. Funding is usually completed with cryptocurrency or any other virtual payment method.
3. *Training.* Recruits' training is often achieved with the utilization of SMPs. After the procedure of engaging users with the purpose of recruiting them, terrorist organizations tutor and train their followers to perform cyberattacks and provoke them to improve their combatting skills.
4. *Planning.* Remote communication is the key to a successful terrorist attack. As terrorists target critical technical infrastructures of their victims, secrecy and flawless coordination are of outmost necessity. In addition, *social-engineering techniques* are deployed, in order to gather vital information, related to the potential target.
5. *Execution.* Every single element described in the above-mentioned categories, may be enacted when it comes to the execution of a cyberterrorism act.
6. *Cyberattacks.* They are performed with the ultimate goal of exploiting the vulnerabilities of the target's computer system, penetrate it and finally, launch the designated attack. *Cyberattacks* may involve acts like *website defacement, Ddos attacks, malware, hacking, etc.*

Concisely, SMPs offer cyberterrorists the means of spreading their vile ideas, more rapidly and efficiently. Hence, LEAs and SMPs have to take drastic shielding countermeasures to protect the public, from these kinds of violent acts.

### 3.1.3 Cyberbullying and Cyberstalking

At some point, every single person has been a victim of bullying or harassment. Bullying is a widely known term, used to explain the *"ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to* *cause physical, social and/or psychological harm"* [86]. The rapid development of SMPs, jointly with the given purpose of every SNS, which is no other than the establishment of online communities through the facilitation of users' communication, have enabled the mass and effortless misbehaviors of bullying violators. SMPs are regularly exploited by bullies, to terrorize, threaten and distress other users. It may seem quite insignificant, but due to the unknown psychological background of the victims, these acts have occasionally led to self-harm, violence and, in extreme situations, suicide [87].

Due to the massive increase of hate speech, through *cyberbullying*, many countries have taken drastic measures in order to prevent these criminal acts and assist victims. In the U.S.A., the *Cyberbullying Research Center*, was launched in 2005 from Dr. Sameer Hinduja and Dr. Justin W. Patchin, to educate adolescents, parents and law enforcers, regarding *cyberbullying* and *cyberstalking* [88]. Moreover, in the United Kingdom (U.K.), the National Bullying Helpline is a charitable organization, founded in 2003 in order to protect and inform the public. According to the U.K.'s organization, *"Cyberbullying is bullying online and any form of anti-social behaviour over the internet or via a mobile device. It is an attack or abuse, using technology, which is intended to cause another person harm, distress or personal loss."* [89]. In addition, SMPs have implemented their own forums and help centers, to help and support victims. In particular "Facebook" has created the *"Bullying Prevention Hub"* [90], which is a portal through which the SNS provides guidance and prevention suggestions on how to take precautions, not only to underage users, but also to their parents.

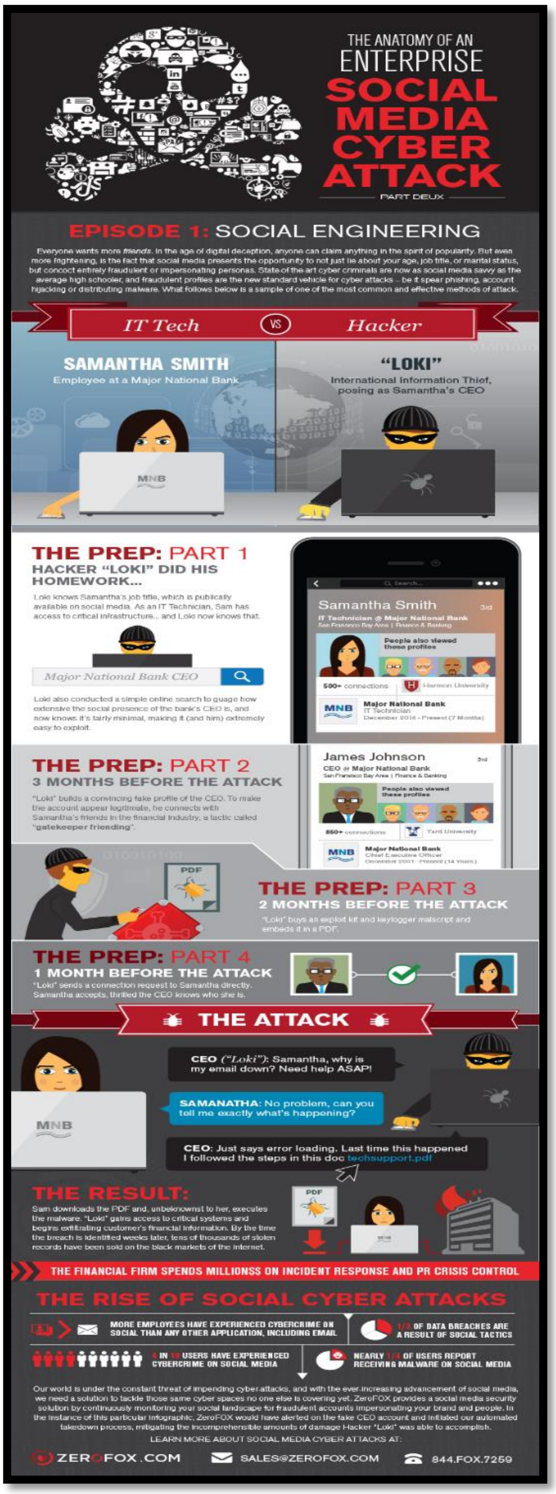
While *cyberbullying* is the broadly accepted term, *cyberstalking* is a deviant behavior that is usually mistaken as an act of *cyberthreat* or *cyberbullying*. Despite the fact that *cyberstalking* definitions vary, a general description of the term is provided by the FBI Law Enforcement Bulletin, as follows: *"The term "cyberstalking" is used to refer to the repeated use of the Internet, e-mail, or other electronic communications devices to stalk, annoy, alarm, or threaten a specific individual or group of individuals"* [91]. Although *cyberstalking* is undoubtedly a main form of *cyberbullying*, it differentiates due to the fact that *cyberstalking* is a behavior which explicitly aims at making the victim feel extremely concerned about his/her safety and causing feelings of emotional anxiety, stress or frustration [92]. Predators tend to cyberstalk their victims, through SMPs, by tracking down their information from their posts, sending them numerous text messages or posting about them, on their personal profiles, without their permission.

### 3.1.4 Social Engineering and Phishing

According to ENISA, *"Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons."* [93]. In plain terms, *social engineering* is the act of obtaining any kind of information, with or without the use of technological skills. Personal information is today's currency. The growth of SMPs and the wide spread of their fundamental services amongst their users (content uploading, provision of personal information, etc.) has facilitated the vast development of *social engineering*. "Scammers" *(i.e., one who perpetrates a scam or a person who commits or participates in a fraudulent scheme or operation* [94]*)*, either use psychological manipulation to gather information related to a future target or deploy specific types of high-tech techniques (e.g. phishing), in order to exploit a user's personal information to obtain unlawful profit (e.g. obtaining credit card credentials, to steal a user's money).

The psychological manipulation of the target usually derives from his/her need of human interaction or the conversational skills of the attacker. From a certain point of view, scammers are talented manipulators who have perfected the art or conversation significantly. Thus, people tend to trust them with their secrets, even though they do not know them in person. The act of *social engineering* does not constitute a criminal act by default, albeit the criminal activity occurs when the obtained information is used in an unlawful way [3]. In **Figure 14**, "ZeroFox SaaS Technology" has created a *social engineering* attack scheme related to a scam, which had taken place against an enterprise. In this scheme, the scammer has deployed specific technological techniques, such as the infection of a common .pdf file, with a *phishing* tool.

*Social engineering* consists of various forms of techniques, such as *pretexting, baiting, quid pro quo* and *tailgating. Phishing/spear phishing* is a more sophisticated technique used for *social engineering*, which requires high-level technical skills, in order to either develop or deploy the appropriate tools. In IC3's annual report, *phishing* is the most frequently reported criminal activity, counting 114,702 victims in the U.S.A. [79].



EPISODE 1: SOCIAL ENGINEERING

Everyone wants more *friends*. In the age of digital deception, anyone can claim anything in the spirit of popularity. But even more frightening, is the fact that social media presents the opportunity to not just lie about your age, job title, or marital status, but concoct entirely fraudulent or impersonating personas. State of the art cyber criminals are now as social media savvy as the average high schooler, and fraudulent profiles are the new standard vehicle for cyber attacks – be it spear phishing, account hijacking or distributing malware. What follows below is a sample of one of the most common and effective methods of attack.

IT Tech
VS
Hacker
SAMANTHA SMITH
Employee at a Major National Bank
"LOKI"
International Information Thief, posing as Samantha's CEO
MNB

THE PREP: PART 1
HACKER "LOKI" DID HIS HOMEWORK...

Loki knows Samantha's job title, which is publically available on social media. As an IT Technician, Sam has access to critical infrastructure... and Loki now knows that.

Loki also conducted a simple online search to guage how extensive the social presence of the bank's CEO is, and now knows it's fairly minimal, making it (and him) extremely easy to exploit.

Search...
Samantha Smith
3rd
IT Technician @ Major National Bank
San Francisco Bay Area | Finance & Banking
People also viewed these profiles
500+ connections
Harmon University
MNB
Major National Bank
IT Technician
December 2014 - Present (7 Months)

THE PREP: PART 2
3 MONTHS BEFORE THE ATTACK

"Loki" builds a convincing fake profile of the CEO. To make the account appear legitimate, he connects with Samantha's friends in the financial industry, a tactic called "gatekeeper friending".

James Johnson
3rd
CEO @ Major National Bank
San Francisco Bay Area | Finance & Banking
People also viewed these profiles
850+ connections
Yard University
MNB
Major National Bank
Chief Executive Officer
December 2001 - Present (14 Years)
PDF

THE PREP: PART 3
2 MONTHS BEFORE THE ATTACK

"Loki" buys an exploit kit and keylogger malscript and embeds it in a PDF.

THE PREP: PART 4
1 MONTH BEFORE THE ATTACK

"Loki" sends a connection request to Samantha directly. Samantha accepts, thrilled the CEO knows who she is.

THE ATTACK

CEO *("Loki")*: Samantha, why is my email down? Need help ASAP!

SAMANATHA: No problem, can you tell me exactly what's happening?

CEO: Just says error loading. Last time this happened I followed the steps in this doc techsupport.pdf

THE RESULT:

Sam downloads the PDF and, unbeknownst to her, executes the malware. "Loki" gains access to critical systems and begins exfiltrating customer's financial information. By the time the breach is identified weeks later, tens of thousands of stolen records have been sold on the black markets of the internet.

THE FINANCIAL FIRM SPENDS MILLIONSS ON INCIDENT RESPONSE AND PR CRISIS CONTROL

THE RISE OF SOCIAL CYBER ATTACKS

MORE EMPLOYEES HAVE EXPERIENCED CYBERCRIME ON SOCIAL THAN ANY OTHER APPLICATION, INCLUDING EMAIL

1/3 OF DATA BREACHES ARE A RESULT OF SOCIAL TACTICS

4 IN 10 USERS HAVE EXPERIENCED CYBERCRIME ON SOCIAL MEDIA

NEARLY 1/4 OF USERS REPORT RECEIVING MALWARE ON SOCIAL MEDIA

Our world is under the constant threat of impending cyber-attacks, and with the ever-increasing advancement of social media, we need a solution to tackle those same cyber spaces no one else is covering yet. ZeroFOX provides a social media security solution by continuously monitoring your social landscape for fraudulent accounts impersonating your brand and people. In the instance of this particular infographic, ZeroFOX would have alerted on the fake CEO account and initiated our automated takedown process, mitigating the incomprehensible amounts of damage Hacker "Loki" was able to accomplish.

LEARN MORE ABOUT SOCIAL MEDIA CYBER ATTACKS AT:

ZEROFOX.COM SALES@ZEROFOX.COM 844.FOX.7259

***Figure 14**: The anatomy of an enterprise - Social Media cyber-attack*

*Phishing attacks* are described as *"a means to persuade potential victims into divulging sensitive information such as credentials, or bank and credit card details."*, while *"spear phishing is a more sophisticated and elaborate version of phishing. It targets specific organisations or individuals and seeks unauthorized access to confidential data."* [95]. Even though *social engineering, phishing* or *spear phishing* techniques can be performed through various systems or platforms, SMPs once more offer a welcoming environment for the utilization of these criminal activities. SMPs' offered communication services, combined with the lack of users' awareness, result in the provision of unlimited resources for online fraudsters and impostors.

## 3.1.5 Malware

*Malware* is a familiar term for most Internet users, and it is a compound word, deriving from the words: *malicious* and *software*. According to ENISA's glossary, *"Any piece of software that performs undesirable operations such as data theft or some other type of computer compromise can be categorized as Malware."* [96]. A *malware* can be installed in a user's computer, without his prior knowledge, and it is used as a technique to reveal personal information. This software reproduces itself and spreads through a network, with the goal of infecting as many machines as possible. SMPs attract criminals who seek to exploit systems with *malware* or *viruses*, as they list millions of users [3].

A basic concept of each SMP is the distribution of content. *Malwares'* and *viruses'* developers hide their destructive code behind (hyper-) links, attachments or messages, which constitute the main body of the shared content. Once a user responds to this content, the *malware* immediately infects the computer in use, as well as any other attached devices [76]. FBI's annual Internet Crime Report for 2019 has reported 2,373 victims of *malware/spyware/virus attacks* [79].

Penetrators have adopted many methods in order to deploy *malware* attacks. The main categories of *malwares* are: *trojan, virus, worm* and *spyware* [96].

1. A *Trojan* or *Trojan Horse* (deriving from the ancient Greek myth of the Trojan War) is a type of *malware* which is disguised by its developer as a legitimate software, in order to persuade the targeted user to install it. As soon as the software is installed in the device, it "runs" the malicious code in the background.
2. *Virus* is the type of *malware* which is attached to a program, a file or any other form of content. Once the victim opens the content or launches the infected program, the *virus* replicates itself and spreads from one device to another. Common practices of a *virus* infection are: Internet downloads, direct messages' attachments or (hyper-) links, executables, etc. The fact that a *virus* requires a human action in order to spread is notable.
3. A *Worm* is similar to a *virus*, due to the fact that both *malwares* spread from one computer to another. The main difference between them, is that while a *virus* requires a human action in order to spread, a *worm* can exploit a system's vulnerabilities, without the former action of the targeted user. The most destructive computer *worms* of all times were: *"ILOVEYOU", "Code Red"* and *"Conficker"* [97].
4. Lastly, a *Spyware* is a *malware* that spies on a user's activities without his prior knowledge or consent. Usually, a *spyware* targets on unlawful data collection, activity monitoring or *keylogging (i.e., a piece of software that records the signals sent from a keyboard to a computer usually for the purpose of gaining information about the user without the user's knowledge* [98] *).*

### 3.1.6 Frauds

SMPs' development has empowered the introduction of all forms of online frauds. Due to the formation of private groups and the ability to interact with other users through personal messages, organized crime has thrived and launched new forms of frauds or scams. *Investment frauds, confidence/romance frauds, credit card frauds, lottery/sweepstakes/inheritance frauds*, along with many more, comprise the majority of online scams conducted through SMPs and specifically through SNSs, like "Facebook", "Twitter", "Instagram", etc.

*Investment fraud* is a relatively new-found type of scam, through which the perpetrator is disguised as a successful investment advisor, eager to assist the potential investor to make large profit. The scam usually begins with an advertisement on a SMP, accompanied with an ostensibly innocent request for a user's phone number or email. Once the users provide their contact information, the scammers get in touch with them, almost immediately. Finally, as the users are reassured that the investments are legitimate and profitable, they send their money straight away, without realizing that they have just lost a fortune [99].

*Romance scams* occur when criminals create fake profiles on SNSs, to track down other users' profiles, belonging usually to either isolated or lonely people, with the intention to lure them into a romantic relationship and embezzle them. Scam artists often pretend to be high-ranking military officers or prominent medical doctors, who seek for money to pay either an urgent medical surgery or an unexpected legal fee [100]. IC3's annual report, counted 19,473 victims of *confidence/romance frauds* [79].

*Credit card frauds* are considered to be a type of *identity theft*, through which criminals use another person's credit card credentials to make unlawful purchases or withdraw money from his/her bank account. IC3 reported 14,378 victims of *credit card fraud*, in 2019 [79].

*Lottery, sweepstakes and inheritance frauds* belong to the same type of scams, for the reason that violators execute them by promising an unexpected and vast amount of money to SNS's users. In exchange, users are simply obliged to pay for tax fees, legal or banking bills, etc. [101]. According to IC3's report, FBI numbered 7,767 victims, in 2019 [79]. Depending on the type of fraud, scammers either claim to be lawyers from overseas, administrating inheritance (inheritance fraud), or officials who are in search of the lottery winner (lottery fraud), or a grand contest's representatives who have called to inform the victim about his/her surprising winning, even though s/he has never participated in any contest (sweepstakes fraud). Unfortunately, the most common victims of these types of frauds are the elderly.

### 3.1.7 Child sexual abuse/ exploitation

SNSs offer the perfect environment for users' interaction and sharing of content. As 2020 is the year in which the whole world has been quarantined, SNSs provide the aspect of communication that lacks from every person's life. While most people tend to use social media to communicate or simply relax, they can easily create a hazardous environment; especially in cases that it is used by people with sexual addictions or problematic behaviors.

Nowadays, all adolescents possess high tech mobile devices and a registered account, possibly on every existing SNS. The exchange of context from one to another by using direct messaging is a daily routine. Whilst others limit the exchange of content in just sending funny photographs, there are teenagers who send pornographic images of themselves, to their mate. *Sexting* is an ordinary phenomenon. It is defined as *"the sending of sexually explicit messages or images by cell phone"* [102].The easiness in which this content is distributed or forwarded to other users, can produce devastating results. Minors do not seem to understand that by sending this kind of photographs, they circulate child sexual abuse/exploitation material.

Another serious problem existing in SNSs is the presence of sexual predators. SNSs' established communities create countless lists of underaged victims for sexual violators. *"Online Grooming is when a predator builds an online relationship with a child by giving compliments or a "shoulder to lean on" or sending gifts until the child trusts the predator."* [87]. *Grooming* is a criminal activity that needs an extended period of time to take place. The trust between the predator and the prey must be built with patience and reassurance. Thus, violators tend to work with multiple targets. When the victim feels comfortable and relaxed with the predator, then there is no turning back. Typically, offenders exploit their victims by either blackmailing them into sending nude content of themselves or performing sexual acts through a webcam. Afterwards, the obtained pornographic material may be distributed or sold to other pedophiles [3].

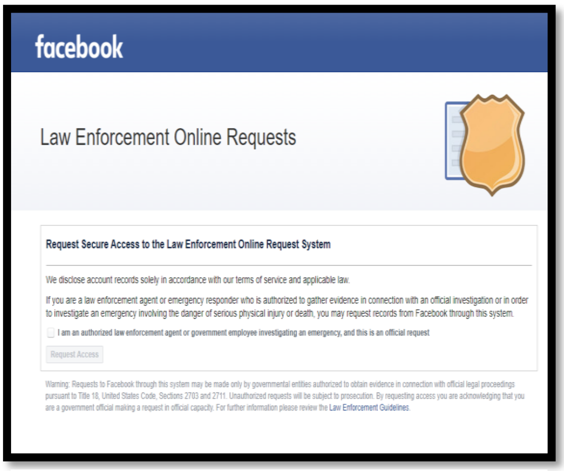
*Child exploitation* and *child sexual abuse* are considered to be the most hideous and shocking criminal actions occurring in cyberspace. As a result, LEAs collaboratively with

SMPs put on a lot of effort to eradicate the phenomenon of child sexual abuse/exploitation.

## 3.2 Information gathering – Intelligence and Enforcement

Crime is a natural consequence of every functional society. Social media consist the cybernetic societies where crime thrives. Above and beyond the provision of innumerable merits, SMPs have greased the wheels for the endorsement of traditional crime to the realms of cyberspace. Criminal endeavors manipulate their users in order to embezzle them, steal their personal data, exploit their computer systems and harass them in any possible way. All in all, cybercriminals abuse SMPs for their own personal benefit.

Therefore, besides LEAs, SMPs ought to take the appropriate countermeasures to protect their users and facilitate the identification of unknown perpetrators. In effect, SMPs have implemented two supplementary types of security measures, apart from informing their users about any potential criminal activity on a daily basis. First of all, SMPs have created their own reporting mechanisms, through which every user can report any impeding violation of the community's terms of service. According to the reported violation, an employee, or an automated process of the SMP probes the grounds of the illicit activity and either bans the violator/user from using the platform or rejects the reporting. Additionally, SMPs have implemented their private portals, as shown in **Figure 15** and **Figure 16**, through which LEAs can request a user's processed data.



Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

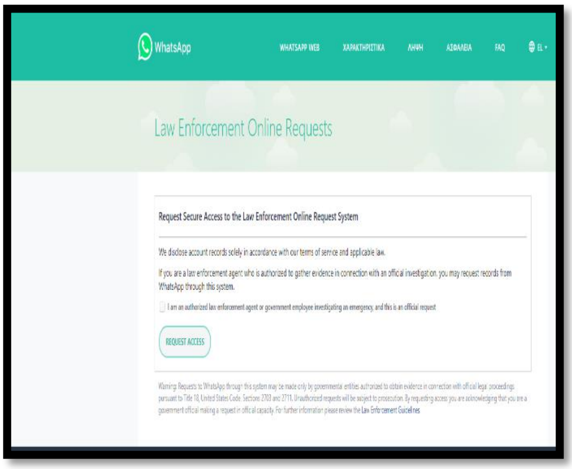
If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.

***Figure 15****: Facebook's online law enforcement platform*



Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from WhatsApp through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

REQUEST ACCESS

Warning: Requests to WhatsApp through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines

***Figure 16****: WhatsApp's online law enforcement platform*

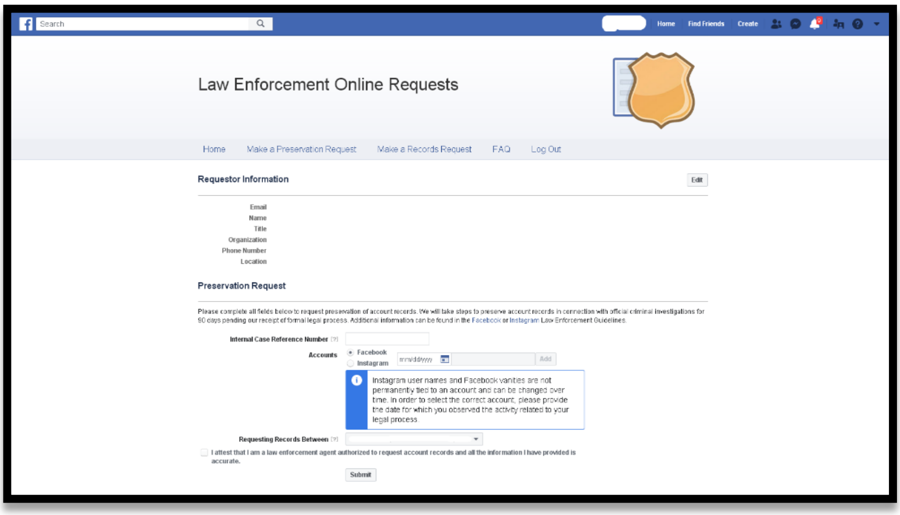
It is highly important to clarify that LEAs cannot request the disclosure of data of every registered user, without the former provision of proper justification. Police agencies' requests must be based on a legitimate ground, followed by a signed legal proceeding and limited to the investigated user. In addition, as most SMPs are established inside the U.S.A.'s territory, every request outside the country's jurisdiction must be submitted either through LEAs' international channels or via the mutual legal agreements, signed amongst countries. There are few SMPs, like "Facebook" or "Twitter", that comply to requests of non-U.S.A. police authorities, based upon their own policies.

In chapter 2, the various types of data that SMPs automatically collect and process from their users have been thoroughly analyzed. Registered e-mail accounts, geolocation information, payment methods and networking data are merely some of them. Nevertheless, despite the fact that a conventional police officer lacking the knowledge of making good use of this information may find it worthless, a cybercrime agent who has been trained to handle various aspects of computer science is more likely to discover an informational goldmine among them.

### 3.2.1 Preservation Request

The U.S.C., Title 18, § 2703 (f)(1), states that *"A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."*. According to the Code, a government official is able to send a preservation request (either through a preservation letter or by using the implemented law enforcement preservation-request platform), in order to demand the SMP to preserve the records of the associated account. The social media entities are obliged to preserve the data that exist at the time when the request is received, but do not retain the records of future provided information. Upon receiving the preservation request, SMPs must keep the preserved records for up to a period of ninety days. Moreover, the government official may ask for a further extension of the preservation period. With any additional request, SMPs must keep the preserved data for another ninety days.

Preservation requests are highly valuable for cybercrime agents. In brief, they initiate the investigation procedures and inform the SMP that a legal action has been taken, due to the previous occurrence of an illegal activity. As SMPs' user accounts are volatile, with the content and the provided information changing instantaneously, law enforcers seek for the preservation of data in order to ensure that evidence or information that may lead to the identification of an unknown perpetrator or the reconnaissance of a criminal activity, is not lost [3]. A preservation request may be submitted in two different ways. Either via the implemented law enforcement preservation-request platform (as depicted in **Figure 17**), or by filling up the preservation letter and sending it to the designated SMP (**Figure 18**).



Law Enforcement Online Requests

Requestor Information

Email
Name
Title
Organization
Phone Number
Location

Preservation Request

Please complete all fields below to request preservation of account records. We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. Additional information can be found in the Facebook or Instagram Law Enforcement Guidelines.

Internal Case Reference Number [?]

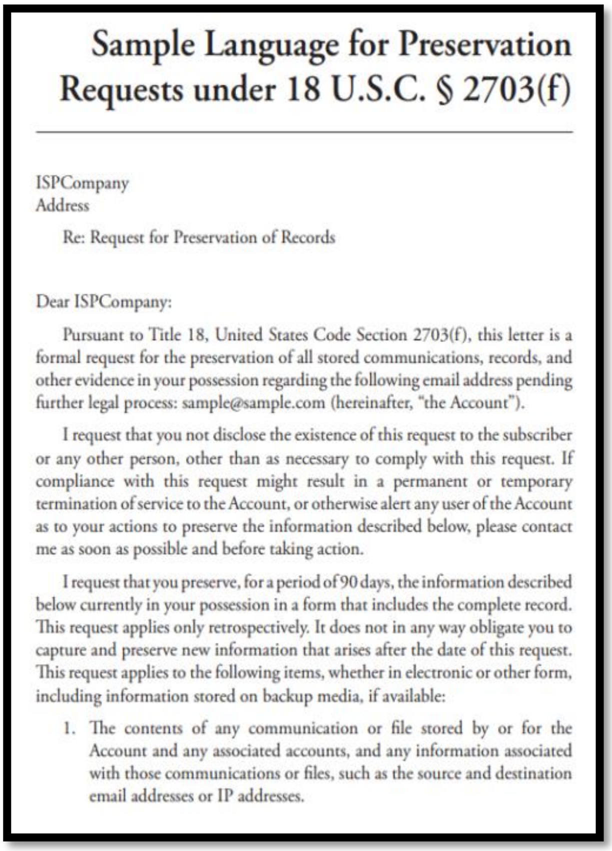
Accounts ● Facebook ○ Instagram mm/dd/yyyy

Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

Requesting Records Between [?]

□ I attest that I am a law enforcement agent authorized to request account records and all the information I have provided is accurate.

***Figure 17***: *Preservation request via Facebook's online law enforcement platform*



Sample Language for Preservation Requests under 18 U.S.C. § 2703(f)

ISPCompany
Address

Re: Request for Preservation of Records

Dear ISPCompany:

Pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following email address pending further legal process: sample@sample.com (hereinafter, "the Account").

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

***Figure 18***: *Preservation request letter*

### 3.2.2 Subpoena

Subpoenas are the most commonly applied legal requests, by LEAs. Police authorities employ administrative subpoenas, authorized by *"a Federal or State statute or a Federal or State grand jury"* in order to disclose information about a SMP's subscriber. A subpoena is defined as *"a written order to compel an individual to give testimony on a particular subject, often before a court, but sometimes in other proceedings (such as a Congressional inquiry). Failure to comply with such an order to appear may be punishable as contempt."* [103]. SMPs require the submission of a valid subpoena, linked to an ongoing official criminal investigation, in order to disclose basic record information. related to a subscriber's account [104]. According to the U.S.C., Title 18, § 2703 I(2), SMPs shall disclose the following information to the competent authority:

1. *Name,*
2. *Address,*
3. *local and long distance telephone connection records, or records of session times and durations,*
4. *length of service (including start date) and types of service utilized,*
5. *telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and*
6. *means and source of payment for such service (including any credit card or bank account number).*

### 3.2.3 Court Order

Court orders are the legal requests through which SMPs disclose the above-mentioned basic subscriber information (provided also through a subpoena), complemented with *"certain records or other information pertaining to the account"* [105]. The additional information provided *"may include message headers and IP addresses"*, but the content of the subscribers' communications is strictly excluded from disclosure. A court order is defined as *"a legal command issued by a judge or other judicial official"* [106].

Even though court orders can provide a lot of information, either for the probed subscriber or for the investigated criminal activity, they are not preferred by the police authorities as they require explicit justification for their issue [3]. Externally derived data found in a SMP's user account may not always provide the solid evidence, which the issue of a court order demands. Therefore, it may be extremely challenging for the investigator to prove that the data of the associated account must be disclosed, due to its connectivity to the investigation. In any case, LEAs have a propensity for taking these risks, as the provided information through the court order, may lead in the identification of the unknown perpetrator [3].

It is clearly stated in many SMPs' law enforcement guidelines that upon receiving of the court order, they may notify the subject of the investigative measures. Nevertheless, in cases where police authorities believe that the suspect's notification could result in jeopardizing the investigation, they can specifically include the prohibition of informing the user/suspect in the issued court order [107].

### 3.2.4 Search Warrant

Cornell Law School defines the search warrant, as *"a warrant issued by the competent authority authorizing a police officer to search a specified place for evidence even without the occupant's consent"* [108] and is required for a search under the *"Fourth Amendment"* [109]. In summary, the *"Fourth Amendment"* states that a law enforcer asking for the issue of a search warrant, must provide the existence of *"probable cause"*, along with an explicit description of the *"place to be searched, and the persons or things to be seized."*. *"Probable cause"* usually exists, either when the current proof indicates the commitment of a criminal activity, or when the vital evidence that confirm the commitment of a crime is present, in the *"place to be searched"*. While considering the fact that SMPs belong to the realm of cyberspace, it is easily understandable that the meanings of the terms, *"place"* or "*things to be seized"*, are quite vague. Hence, although probable cause is still a prerequisite for the issue of a search warrant, SMPs require the description of messages, photos, videos, timeline posts, and location information [105], instead of the clarification of a *"place"*, in order to accept the legal proceeding and disclose the requested data.

### 3.2.5 Requests from Foreign Authorities – Law correlation

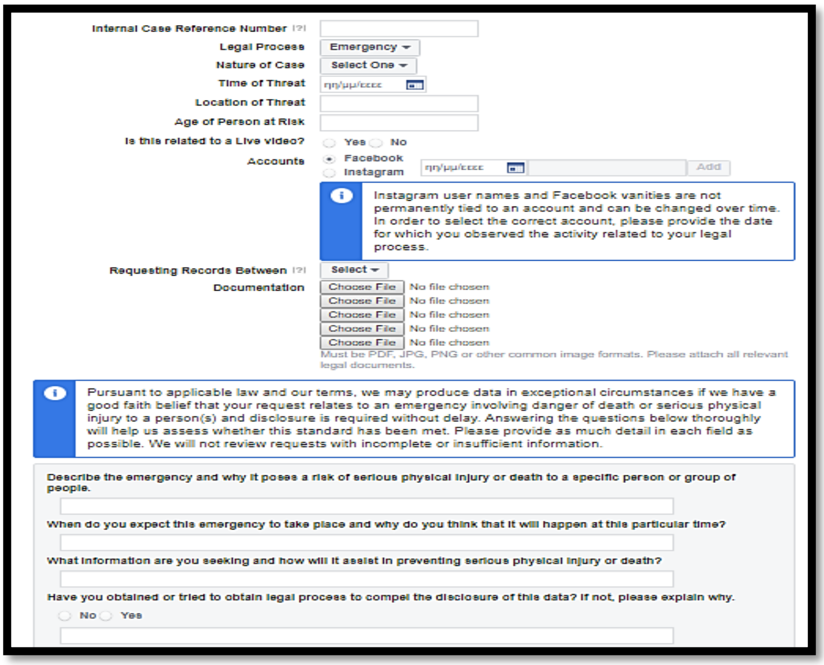
SMPs' provided services, attract people from all over the world. Consequently, criminality on SMPs meets no physical borders. Violators, from any geographical location of our society, use and exploit SMPs' systems, in order to fulfil their illegitimate purposes. To this extend, it is easily comprehensible that it is not only U.S.A.'s LEAs who seek for assistance from SMPs. As perpetrators may reside anywhere around the world or, in addition act harmfully against any person globally, the fact that SMPs provide their aid to any kind of LEA worldwide should be considered highly crucial. Indisputably, there are many prerequisites which ought to be met by the foreign LEAs, such as the formality of the requests or the correlation of Law violations, between the national Laws of the "requesting authority" and the jurisprudence that abides the "receiver" SMP. As most SMPs have their core establishments in the U.S.A., the "Law correlation" refers to the correlation between the contextually national Law and the U.S. Code.

There are three approaches, in which foreign LEAs may enquire for users' data from SMPs. Initially, police agencies can send a formal request to the competent national authorities, via the international police channels (e.g., INTERPOL). However, under the applicable law, SMPs demand a signed legal proceeding in order to disclose users' data. Subsequently, non-national authorities may enquire an issue of such a proceeding through formal requests [105], specified as a "Mutual Legal Assistance Treaty request" or "letter rogatory". Nevertheless, as both practices, formal legal requests and interaction through international channels necessitate tons of paperwork and time-consuming bureaucracy, many SMPs have developed their own law-enforcement platforms, through which LEAs can communicate directly with them. In any case, as the uncontrolled and unlawful disclosure of users' data in any police authority is illegal, it is still requested that the LEAs, intricately inform the SMP regarding the ongoing investigation, as well as to provide a national signed legal proceeding.

### 3.2.6 Exception – Emergency Data Request

In explicit situations, either when there is an imminent threat of physical injury against individuals or missing person cases, SMPs have implemented specific procedures through which LEAs can request for an immediate disclosure of users' data, in order to prevent the occurrence of such situations, without further delay [105]. Cases in which SMPs may provide directly the requested data are called *"emergency cases"* and usually involve child safety incidents, kidnaps of adults/minors, suicides, physical assaults and terrorist activities. Through the "emergency data request", SMPs do not demand the provision of a signed legal form, as it is considered extremely time-consuming and could possibly result in the occurrence of the emergency.

In any case, as depicted in **Figure 19**, SMPs demand a detailed justification in order to disclose the requested data. The handler of the case, who is usually a law enforcement official, must provide specific details which distinguish a case as an emergency. Information regarding the nature of the case and how the provided data would assist in the prevention of the emergency are of outmost necessity. However, as this procedure relies upon the good faith of the SMPs, if the law enforcement official fails to provide the proper justification or proof, that would characterize the case as an "emergency", SMPs may refuse to disclose the requested information.



Internal Case Reference Number [?]

Legal Process: Emergency

Nature of Case: Select One

Time of Threat: ηη/μμ/εεεε

Location of Threat

Age of Person at Risk

Is this related to a Live video? ○ Yes ○ No

Accounts: ● Facebook ○ Instagram ηη/μμ/εεεε

Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

Requesting Records Between [?]: Select

Documentation: No file chosen

No file chosen

No file chosen

No file chosen

No file chosen

Must be PDF, JPG, PNG or other common image formats. Please attach all relevant legal documents.

Pursuant to applicable law and our terms, we may produce data in exceptional circumstances if we have a good faith belief that your request relates to an emergency involving danger of death or serious physical injury to a person(s) and disclosure is required without delay. Answering the questions below thoroughly will help us assess whether this standard has been met. Please provide as much detail in each field as possible. We will not review requests with incomplete or insufficient information.

Describe the emergency and why it poses a risk of serious physical injury or death to a specific person or group of people.

When do you expect this emergency to take place and why do you think that it will happen at this particular time?

What information are you seeking and how will it assist in preventing serious physical injury or death?

Have you obtained or tried to obtain legal process to compel the disclosure of this data? If not, please explain why.

○ No ○ Yes

**Figure 19**: *Emergency Request via Facebook's platform*

## 3.3 Investigations through Social Media

Up to this point, we have thoroughly analyzed the implemented data disclosure platforms and legal proceedings, that SMPs have adopted in order to assist LEAs in identifying unknown online perpetrators. It can be easily concluded that SMPs, in accordance with the applicable law, have introduced all the appropriate mechanisms, analogous to every possible situation; either in times when the case involves an ongoing criminal investigation or an imminent threat of physical injury, SMPs will provide a user's recorded data requested by the competent authority. At this point, it is important to explain that apart from the legitimate provision of users' data, SMPs are considered to be information goldmines in the hands of an experienced and skilled cybercrime investigator. By deploying the suitable programs and investigating techniques, LEAs are capable of retrieving copious evidence related to a criminal activity [110].

In chapter 2, we have thoroughly described the types of data that an average user may upload on his/her personal account. Even though criminals who create and use accounts on any SMP, are way too careful, regarding their shared content, there are specific data that can be obtained by a cybercrime agent and may possibly lead in the identification of the unknown perpetrator. Even if the investigated user/criminal has only one "friend" on his "Friend's" list, a "reverse lookup function" may provide several information for the user at issue [111]. Furthermore, users' profiles may easily provide several hidden "artifacts", like pictures' metadata or geolocation activity, which after being processed by the deployed software or open-source techniques, they can offer useful information. Publicly available information can be used in examining a criminal actor's social or illegitimate activities. These sophisticated practices, along with the disclosure of a user's private information from SMPs, can lead to the detection of unidentified violators and the solution of numerous unsolved criminal cases [110].

Another major advantage that an online investigation of a user's profile may provide is the so-called *"Social Media Profiling"* or *"behavior prediction"*. *"Profiling"* is a concept, mostly related to the prevention of all kinds of criminal activities, rather than the identification of criminals' identity *per se*. The extraction of personal information from a user's profile may possibly lead to the prevention of a crime or, in many cases, the prevention of situations where the investigated user tends to harm himself/herself. In any case, as "behavior prediction" derives from the analysis of a user's personal provided content, LEAs must be very careful on how they use these practices. An individuals' constant surveillance, who has not acted harmfully yet, can be characterized as an exploitation of his/her social life. Thus, the investigated profiles must belong to users who either have a felonious record or belong to a group of people who are known for their criminal background [8]. In legal terms, the investigator must provide a "probable cause" in order to examine a user's profile in any way. It has to be clarified that data processing occurring through *"Profiling"* is neither unlawful nor arbitrary. In the following subsection, the legal grounds upon which *"Social Media Profiling"* procedures are legitimately deployed will be briefly analyzed [112].

### 3.3.1 Open-Source Intelligence (O.S.INT.)

Before analyzing O.S.INT. for LEAs' investigations, it is essential to understand what open-source intelligence actually involves. *"Open-Source Intelligence (OSINT) is a concept to describe the search, collection, analysis, and use of information from open sources, as well as the techniques and tools used. OSINT emerges out of a military need to collect relevant and publicly available information."* [113]. As the definition states, O.S.INT. is the method of extracting information from open sources, like the Internet, traditional mass media, photographs, etc. [114]. In general terms, these techniques are used in order to gather information related to an individual or the subject at issue. While O.S.INT. can be applied in any kind of means that provides content, cybercrime LEAs tend to utilize these methods on SMPs' users' profiles, as they provide various information, in plain sight. It must be clarified that open-source gathered data, do not involve information that: *"is classified at its origin, is subject to proprietary constraints (other than copyright), is the product of sensitive contacts with U.S. or foreign persons, or is acquired through clandestine or covert means"* [115]. In any case, O.S.INT. practices do not require a user's consent or prior knowledge, in order to extract or process the desired information.

O.S.INT. supports the intelligence and investigation practices deployed by LEAs, in order to gather information that are not protected by privacy restraints. While the police investigators must manually indicate the searching and data crawling criteria, automated processes (i.e., software) retrieve the coveted information. Contrariwise, whenever a LEA's data analyst cannot predetermine the searching criteria, s/he may manually perform the O.S.INT. techniques on a user's profile, in order to verify the existence of usable information and deploy the desired software in later stages. Some of the most known O.S.INT. tools/software are namely: "Maltego", "Recon-ng", "theHarvester", "Shodan" and "IntelTechniques". In addition, there are plenty O.S.INT tools, developed by private companies and used explicitly for data gathering from SMPs, like "Geotweet", "FB Scan Tool" and "Google Plus Search" [116].

As LEAs are engaged in both prevention and investigation of criminal activities, data gathering is of outmost necessity. A police agent's primary goal is to prevent the crime before its occurrence. For instance, a "Twitter's" user public message declaring his/her plan to cause a riot or sell illegal covid-19 drugs on "Facebook" are data that can be gathered through O.S.INT. and can possibly lead to the prevention of other violations.

CCUs have reported many incidents, where SMPs' users have announced their intention to commit suicide and were saved due to the existence of these techniques. Even if on some occasions, the public messages or uploaded content related to an imminent threat, have proven to be fraudulent or intended as jokes, data gathering through these practices has provided a lot of benefits and has literally saved numerous lives [115].

As priorly mentioned, data gathered through O.S.INT. can be also used for investigative purposes and the legal prosecution of perpetrators. By using the information extracted from SMPs' accounts, cross-referenced with other data collected by public archives and investigation techniques (traditional policing), LEAs may gather the necessary evidence to arrest and legally prosecute a criminal violator. From a police agent's perspective, the most challenging part of an investigation is the gathering of evidence that may possibly result in the legal prosecution of a criminal. Content shared through SMPs' accounts is considered to be public data. In addition, content exchanged between two users or in a SMP group, may also be considered public, if one of the sharing users hands over it to LEAs. Evidence gathered through O.S.INT. is legit, as long as it is considered public and not forcibly extracted by the user-violator, with illegal means. Subsequently, one may easily jump to the conclusion that O.S.INT. techniques are utterly important. They provide content and information in an aggressive way, which would be impossible to be gathered in any other way [115].

The issue that may arise from the extensive use of O.S.INT. software derives from the fact that these kinds of technologies are produced by private companies. For instance, "NiceTrack Open-Source Intelligence" is a tool developed by "Nice Ltd", an Israel-based company, that "assists" LEAs and other intelligence organizations by using *"mass interception solutions"*. The software provided by "Nice Ltd", retrieves relations and conversation content, through telephony, IP and satellite [117]. While the "Nice Track Open-Source Intelligence" products are developed specifically for LEAs, there other companies that produce different types of O.S.INT. tools and are available to everyone. Data acquired through these types of software, are usually considered to be private by the users that unwillingly provide them, but in reality, they are publicly accessible either from the private companies that develop them or from the average users that apply them. The development of new information technologies, involving data gathering through O.S.INT., is considered to be extremely important for LEAs, due to the fact that they can possibly minimize all types of cyber threats. Nevertheless, the fact that users' private data are distributed to third-part companies and everyday users is an issue that can potentially grow a lot of legal concerns [115].

The implementation of O.S.INT technologies and their introduction to LEAs circles is yet in a developmental stage. There are two main reasons that impede the full implementation of these techniques. First of all, many officials have raised their concerns regarding the social costs. Virtual communities were created in order to provide users with a safe environment, where they can confine their thoughts and socialize with others, without being surveilled by anyone. In a way O.S.INT. obliterates this essence of communicational privacy and enforces an online monitoring among SMPs. Truly, the idea behind this concept is to guard users against criminals. But the question remains. Who can amenably determine whether online surveillance through O.S.INT exceeds its purpose [115]? In addition, law enforcement agents are not yet qualified to either process the acquired information or handle the deployed software. As SMPs are continuously changing their interfaces in order to satisfy their users, police agents involved in data gathering are obliged to follow these changes. Many LEAs around the world are proclaimed to be understaffed or handled with too many responsibilities. Hence, the endless training on O.S.INT. tools and techniques is deemed a luxury that many LEAs simply cannot afford.

### 3.3.2 Social Media Profiling

SMPs, by their nature, encourage their users to express their thoughts and create groups in their digital worlds. Apart from communicating with others, SMPs provide services through which users can share content, by exchanging and redistributing all kinds of information. "Netizens" become members of large online communities and socialize with others, with whom they share common opinions, interests, religious or political beliefs, etc. Social relationships are the key aspects of all SMPs, as users expose their personalities and share information related to their everyday lives. Nowadays, it seems more rational for someone to reveal his/her private thoughts on his/her "Facebook" account, rather than expressing them to a close friend. According to the uploaded content or disclosed personal information, "Friends" lists or most viewed videos, users can be categorized and clustered in different groups, depending on their social, economic, religious, political or any other possible, statuses. This categorization is called *"Users' Profiling"* or *"Social Media Profiling"* and can be utilized for various purposes, like targeted advertising, maximizing a SMP's user experience, building of social relationships, threat prediction or cyber forensics analysis [8].

*"Criminal Profiling"* is defined as *"a technique whereby the probable characteristics of a criminal offender or offenders are predicted based on the behaviors exhibited in the commission of a crime."* [118]. While this forensic technique is applied in most conventional investigating practices, modern cybercrime investigators have tried to implement it on various occasions. "Criminal Profiling" in traditional police investigations, relies on tangible evidence and constant surveillance of the suspects at issue. *"Social Media Profiling"* for police investigations, seems quite feasible, due to the fact that users/criminals tend to share and expose the desired information on their own. As mentioned above, users register in SMPs with the outmost goal of sharing content and private data. Thus, an investigator who is keen on criminal-profiling methods, can easily extract the desired data and predict possible threats or forthcoming criminal activities. Nevertheless, the process of online "Criminal Profiling" is much more challenging, as digital evidence can be forged by the violator. This fact can ultimately jeopardize the whole police operation [119].

Users' shared content and private information offer a considerable amount of useable information, that would be obscured in any other way. LEAs seek to extract it in order to discover possible correlations or patterns, associated with any impending threat. Police agents employed in the field of "Criminal Profiling" aim to "connecting the dots", by mining the voluntarily provided information. Depending on the patterns, users are assigned and clustered in specific categories. In later stages and after the classifications, LEAs try to predict misbehaviors that may trigger disastrous results. For example, hackers are categorized as *"white, middle-class, obsessive antisocial males between 12 and 28 years old, with an inferiority complex and a possible history of physical and sexual abuse"* [120]. It is quite noticeable, that an individual's personal characteristics, like the age or the economic status, can be easily extracted by the provided content and the personal information existing on a user's account on any SMP. Even though stereotyping felons by studying past offenders is not actually valuable for an investigation, the classification of users according to their criminal past or correlation with other criminal users, may provide the motives that will possibly provoke any forthcoming malevolent behaviors.

The ultimate purpose of “Social Media Profiling” in cybercrime investigations is to identify and understand the criminal. As cybercriminals are keen on hiding their trails, the above-mentioned practices are not deemed as simple as they appear to be. The role of the investigators who are engaged in “Social Media Profiling” is not to unravel the mystery of the crime itself, but to assist investigators in piecing together the collected evidence. Through profiling methods, LEAs attempt to discover the links between criminals and criminal activities. The “cybertrails” *(i.e., a trail of evidence, etc., on the Internet or in cyberspace* [121]*)* collected after the occurrence of a criminal activity, accompanied with the statistical analysis and the categorization of suspects/users may easily bridge the gap in many cold cases. The analysis of the “modus operandi” *(i.e., a distinct pattern or method of operation that indicates or suggests the work of a single criminal in more than one crime* [122]*)* and the identification of the motives behind the criminal act, can reveal the personality of the perpetrator. In general, profiling can produce frameworks, which will set the examples for future recognition of potential online criminal actors [123].

Apart from extracting users’ data, “Social Media Profiling” demands constant observation and surveillance of the user under investigation. Governments and LEAs are on many occasions accused of violating the fundamental rights of individuals. Users may be stigmatized and classified in groups, according to their everyday activities, personal likes and dislikes, etc. “Social Media Profiling” means that the user who is being analyzed and categorized will be subjected to further official or unofficial police investigation. Irrational profiling or utilization of these practices, by untrained investigators, may possibly lead to the phenomena of social inequality and prejudice against minorities or underprivileged groups [8]. Overall, “Social Media Profiling” in cyberspace is a valuable “tool”, which must be treated with caution and handled by experienced police investigators.

In sum, as all stages of “Social Media Profiling” constitute processing of users’ personal data and are deemed “automated decision making” techniques, they are legislated by the LED and in specific by the Article 11(1), which explicitly states that: *“Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.”*. Hence, apart from all above mentioned, LEAs must be extremely careful on how they implement these practices. It is crucial that the police agents, in charge of handling "Social Media Profiling" procedures, rely solely on automated processes (i.e., software) for the "decision making" analysis, in order not to fall out of the scope of the jurisprudence [112].

### 3.3.3 Social Cyber Forensics

Due to the endless and almost uninterrupted development of information technology, cybercrime's explosion is deemed to be uncontrollable. Cybercriminals are equipped with tools and various mechanisms on the Internet, as in the real world, that make their detection and prosecution challenging for most LEAs. The collection of evidence in cyberspace, along with the investigation of cybercriminal activity is very complicated and apart from many years of experience, it requires a deep knowledge of the cyberspace itself. Hence, specialized police agents and professional engineers have implemented "cyber forensics", in their fight against cybercrime. *"Cyber forensics"* or *"digital forensics"*, is defined as *"the process of acquisition, authentication, analysis and documentation of evidence extracted from and/or contained in a computer system, computer network and digital media."* [124]. "Digital forensics" is a continuously evolving scientific field that involves numerous techniques. Namely, some of them are: "cross-drive analysis", "live-analysis on volatile data", "recovery of deleted files" and "stochastic forensics" [125].

One of the most critical stages of a criminal investigation, is the acquisition of evidence, that either identifies the unknown perpetrator, or verifies the existence of a criminal activity. "Cyber forensics" is the field of expertise that is utilized by LEAs in order to gather and analyze the data that will be potentially used in a legal trial. "Cyber forensics" is not a brand-new scientific field. It has been applied in LEAs for over three and a half decades and the tools employed by the police agencies have evolved a lot through all this time. The first digital forensic tools can be traced back in the early 1980s, when they were mostly used by government agencies. Since then, software engineers have made a great progress in order to make them more advanced. Nowadays, they are used in both public and private sector, for reasons of data gathering. Furthermore, modern digital forensic software provides its user with a plethora of visualization capabilities, which make the procedure of analyzing information, much more easier [126].

"Social Cyber Forensics" (SCF), is a specialized "digital forensics" field of expertise, applied on SMPs, and is defined as *"as a branch of cyber forensics which is the process* *of investigating the relationships among "entities" and revealing the digital connections among them in social media space by extracting/collecting metadata associated with their social media accounts, e.g., affiliations of the user, geolocation, and IP address."* [127]. According to this definition, an *"entity"* is any individual, organization, or group, that can be considered as an information provider, such as a SMP user [127]. SCF tools can collect data from SMPs in various ways. For example, forensics investigators can employ certain types of software or specific tools, to gather the information they seek, like collecting information by using "Application Programming Interfaces" (APIs), crawling data/artifacts from local web browser cache or sniffing on unencrypted Wi-Fis (active attacks). Additionally, other designated investigative practices, for data acquiring, involve collecting metadata from SMPs' profiles, like IP addresses, timestamps, geolocations, registered personal information, relationships and affiliations, etc. Usually, metadata acquiring is achieved by using specific forensic tools, but on some occasions more skilled investigators prefer a hands-on approach [126].

For a forensic analyst to be able to retrieve the required data and to determine the relationships and affiliations among the various "entities", the existence of a "seed" is essential. "Seed" is an "initial knowledge", which is used in order to scrutinize an entity. A "seed" can be any kind of information which can uniquely identify an entity; from IP addresses, to "Facebook" accounts or web tracker codes (WTC). In general, a "seed" is the information that a SCF tool requires, in order to initiate the examination and reveal the concealed data related to the investigated entity [127]. For example, a "seed" can be a "Facebook" account's URL, as it can uniquely identify the user of the profile.

At this point, it is extremely important to mention that O.S.INT and SCF techniques are in a certain way codependent. Traditional forensic practices necessitate the actual existence of the physical evidence, which are to be examined. With the extensive use of SMPs, users/criminals provide the desired evidence and data on their personal accounts [128]. Thus, LEAs can obtain the necessary information via O.S.INT. and analyze it with SCF. To this extend, many tools developed for SCF investigations, are also deployed for O.S.INT. practices. For instance, Maltego, which is a tool widely used by all LEAs, was developed for both O.S.INT. and SCF reasons [126]. At first, the aforementioned tool collects a vast variety of data from unlimited open sources and then, it analyzes the real-world interconnections of the data, between all possible entities, from different SMPs like "Facebook", "Twitter", etc.

# 4 Inside a Cyber Crime Unit – The Hellenic Paradigm

The Hellenic Cyber Crime Division (CCD), which is established in Attica Greece, reports to the Hellenic Police Headquarters and is supervised and monitored by the Chief of the Hellenic Police. Its local jurisdiction extends throughout the Hellenic territory. The mission of the CCD is the detection, investigation and prosecution of criminal offenses committed either through the Internet or through other means of electronic communication and digital storage mediums. In particular, the Agency's mission involves the detection and prosecution of crimes committed against minors, as well as the handling of cases regarding illegal intrusions and destruction/alteration or illegal circulation of software, hardware, digital data and audiovisual means, throughout the country. Moreover, the CCD provides assistance to the competent state's authorities in order to prevent suicides announced via the Internet, as well as to other authorities that investigate cases of financial crimes, and in particular, crimes committed against the financial interests of the public and national economy in general, or show the characteristics of organized crime, in accordance with the applicable legislation. The mission of the Cyber Crime Subdivision of Northern Greece (CCSNG), which is based in Thessaloniki, is identical to the central CCU's mission and its jurisdiction extends to the region of the General Division of Security of Northern Greece.

During 2019, the LEA has developed numerous actions, regarding both the prosecution of crimes committed via the Internet and informing the country's citizens about issues related to browsing Internet safely. Moreover, the CCD has cooperated with other competent authorities of the Hellenic Police (Public Security Division, Forensics Investigation Division, Division of Information Management and Analysis, Training and Human Resources Development Division, etc.). The participation of the Division's police agents, in various training seminars of the European Union Agency for Law Enforcement Training (CEPOL), EUROPOL and INTERPOL, as well as in meetings, conferences and symposiums organized by European and international organizations, and held either in Greece or abroad, is highly increased. The Division also participates in the following international actions:

i. in the International Police Operation to Combat Card Fraud in the Aviation Sector (GAAD - Global Airport Action Days),
ii. in the International Police Operation to Fight Card Payment Fraud in the E-Commerce Sector (eCommerce Action), under the coordination and support of EUROPOL, and
iii. to the European Money Mule Action (EMMAV), with the support of EUROPOL, Eurojust and the European Banking Federation (EBF). [129]

The implementation of the "Cyber Alert" Internet Risk Management Center, which operates on a 24-hour basis and where specialized police officers of the Division report citizens' complaints, is quite remarkable. This information, along any other complaints, are submitted either through the Division’s call center, via e-mails, or through the Division’s developed digital applications for mobile devices "Cyberkid" and "Feel Safe" or even through the web portal of the Hellenic Police, where citizens, businesses and organizations have the opportunity to submit complaints, related to any form of electronic crime (e-crime). With this modernized operation of the "Cyber Alert" center, the immediate service and information of the citizens is attempted. This way, people are provided with the opportunity to choose between various ways of communication with the CCD remotely and at any time. From 01/01/2019 to 31/12/2019, a total of one thousand, one hundred and twenty-three (1,123) cybercrime complaints had been submitted, while one hundred and eight thousand one hundred and sixty-three (108,163) calls were received by the call center of the LEA [129].

During 2019, the CCD handled five thousand one hundred and seventy-eight (5,178) criminal cases. Specifically, the LEA investigated three hundred and twenty-nine (329) cases related to child sexual abuse and sexual exploitation of minors through the Internet. Statistically, 39% of the victims were under 15 years old and 61% over 15 years old, while 82% of the victims were female. Also, 17% of the perpetrators were minors (aged 12 years), while 83% of the perpetrators were adults, aged 18 to 87 years. Finally, 90% of them were male. In **Table 1,** the above-mentioned statistics are analyzed in detail [129].

***Table 1:*** *Criminal Cases and related offences.*

| Category | CCD | CCSNG | Total |
|---|---|---|---|
| Internet Fraud / E-Commerce | 1.547 | 228 | 1.775 |
| Personal data / Threat / Defamation | 829 | 156 | 985 |
| Illegal access & Obstruction of operation of information systems / Data Spying / Violation of privacy of communications, etc. and related offenses | 192 | 46 | 238 |
| Child sexual abuse & Sexual Exploitation of Minors via the Internet | 293 | 36 | 329 |
| Animal protection legislation | 156 | 14 | 170 |
| Intellectual property and subscription services offenses | 13 | 4 | 17 |
| Gambling and online betting | 15 | 4 | 19 |
| Intention for commitment of suicides | 340 | 30 | 370 |
| Citizens' requests | 500 | 174 | 674 |
| Assistance to local authorities | 307 | 207 | 514 |
| Assistance in disappearance cases | 32 | 9 | 41 |
| National Security / Espionage / Terrorism (via Internet) | 4 | 0 | 4 |
| Racism / Hate speech online | 22 | 1 | 23 |
| Advertising, circulation of drugs, medicines and related illicit drugs online | 18 | 1 | 19 |

In the context of international police cooperation (INTERPOL, EUROPOL, SIRENE), the Division received and handled one thousand, two hundred sixty-eight (1,268) cooperation requests. There were requests posed related to cases of transnational cybercrime police investigations, requests by domestic authorities for the investigation of crimes committed on the Internet, requests by foreign authorities for crimes committed via the Internet (through EUROPOL-INTERPOL), requests in order to provide assistance to Europol's European Union Internet Referral Unit (EUIRU), and requests posed for providing assistance to either the competent state's judicial or police authorities on terrorism matters.

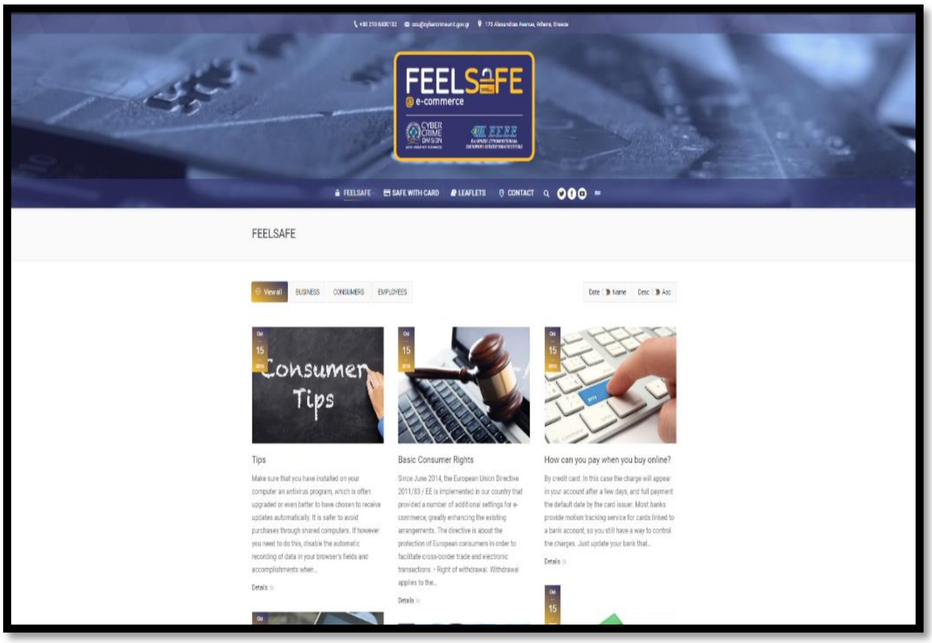
Totally, in 2019, the CCD and the CCSNG, have both arrested and criminally prosecuted thirty-nine (39) people, as depicted in **Table 2** [129].

***Table 2:*** *Arrests of the CCD.*

| Criminal Offence | Arrested |
|---|---|
| Gambling and online betting | 2 |
| Intellectual Property | 3 |
| **Fraud/Computer Fraud** | 1 |
| Child sexual abuse/exploitation | 27 |
| Personal Data | 2 |
| Illicit drugs online | 1 |
| Circulation of drugs/ medicines | 1 |
| Criminal cases related to antiquities | 1 |
| Criminal cases related to weapons | 1 |
|  | Total 39 |

Executing the mission of the Hellenic Police, which is the prevention and eradication of criminality in general, the Hellenic Police Headquarters and the Cyber Crime Division have developed a set of innovative actions. These actions are considered to be important pillars in the prevention and fight against cybercrime. What is more, they totally strengthen the field of engagement of the Hellenic Police in order to embrace society. To this extend, the CCD organizes workshops and lectures throughout Greece, aiming to inform students, parents, educators, consumers, traders and entrepreneurs about the risks associated with new technologies, online shopping, cyberbullying, and to address the dangers lurking on SNSs, etc. In summary, during 2019, the Division organized and carried out five hundred and fifty-two (552) lectures throughout Greece.

Additionally, the CCD has developed its own websites, titled “CyberAlert” [130] and “Cyberkid” [131] (**Figures 20** and **21**), through which the Agency provides counselling to the citizens about the safe use of the Internet in commercial transactions and online shopping. Also, the latter website, which is addressed to children and parents, provides useful information and tips for adolescents, teenagers, families and teachers on how to safely take advantage of the benefits of the Internet and to minimize any potential risks. Moreover, the public can be thoroughly informed about the dangers and the trends in the field of cybercrime, on an exponential basis. It is worth mentioning that the CCD has also implemented two applications for smartphones, namely *Cyberkid* and *Feelsafe*, which have been both developed by the police force’s specialized personnel [129].



FEELSAFE

Tips

Make sure that you have installed on your computer an antivirus program, which is often upgraded or even better to have chosen to receive updates automatically. It is safer to avoid purchases through shared computers. If however you need to do this, disable the automatic recording of data in your browser's fields and accomplishments when...

Details »

Basic Consumer Rights

Since June 2014, the European Union Directive 2011/83 / EE is implemented in our country that provided a number of additional settings for e-commerce, greatly enhancing the existing arrangements. The directive is about the protection of European consumers in order to facilitate cross-border trade and electronic transactions. - Right of withdrawal. Withdrawal applies to the...

Details »

How can you pay when you buy online?

By credit card. In this case the charge will appear in your account after a few days, and full payment the default date by the card issuer. Most banks provide motion tracking service for cards linked to a bank account, so you still have a way to control the charges. Just update your bank that...

Details »

***Figure 20****: CyberAlert website*

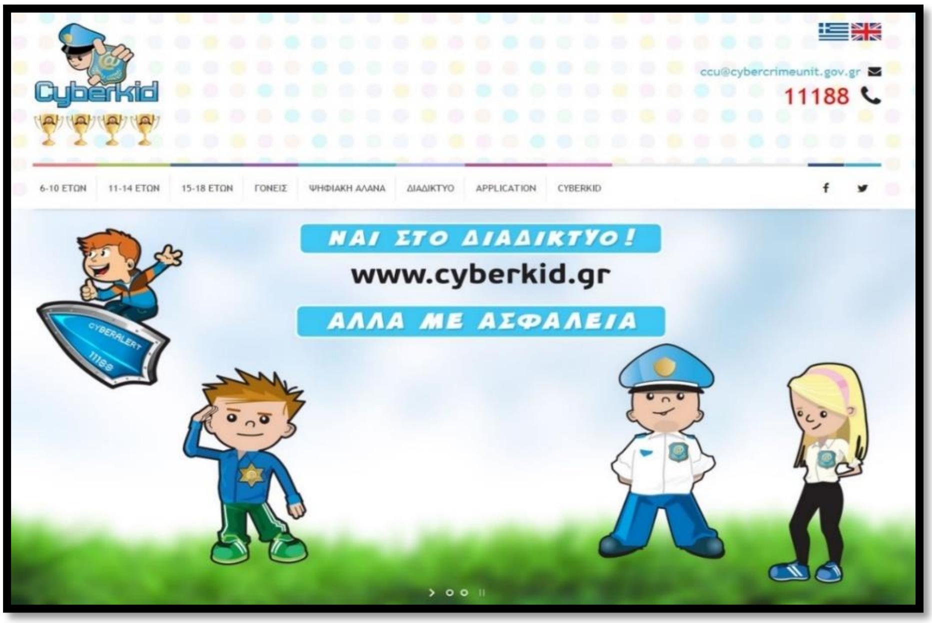


***Figure 21:*** *Cyberkid website*

Likewise, along with the purposes of advising and providing information to the public, the Division has created accounts on various SMPs, such as “Facebook”, “Instagram”, “YouTube” and “Twitter”. The Agency has taken advantage of the merits offered by the SMPs, in order to engage with the Hellenic society in numerous ways, like interacting with the citizens, protecting them from any possible cybercrimes and directly receiving information regarding any emergency situations. Namely, the Division’s accounts on SMPs are: “Facebook” accounts *“Cyberkid”* and *“CyberAlert”*, “Instagram” account *“@cyberalert.gr”*, *“Twitter”* account *“@CyberAlertGR”* and the “YouTube” channel *“Cyber Alert”*.

## 4.1 Structure of the Hellenic CCD – Roles and responsibilities of the Departments

As it has been already mentioned, the Hellenic Cyber Crime Division is based in Attica Greece, its local jurisdiction extends throughout the Hellenic territory and it is structured into the following Departments:

1. *Department of Administrative Support and Information Management,*
2. *Department of Innovative Actions and Strategy,*
3. *Department of Electronic and Telephone Communications Security and Software and Copyright Protection,*
4. *Department of Internet Protection of Minors,*
5. *Department of Investigation of Financial Crimes, and*
6. *Department of Special Affairs and Digital Investigation.*

Every Department has its own responsibilities and deals with specific types of criminal activities and investigations. In detail:

1. The responsibilities of the *Department of Administrative Support and Information Management* are the following:
   - 1.1. the handling of personnel issues, the management of financial issues and material, the secretarial, administrative and technical support and in general, the service of the operational needs of the Police Agency,
   - 1.2. the collection, study, analysis, evaluation, correlation and processing of information, as well as any other data related to the mission of the Police Agency, and the transmission of the processed data to the competent Departments of the Division for operational use,
   - 1.3. the care for the continuously specialized training of the staff of the Division in matters of investigating cybercrime, through the preparation and implementation of educational programs, according to the relevant needs of the operational Departments and in collaboration with the Division of

Training and Development of Human Resources, along with all other competent authorities of the country and of other nations, through the Division of International Police Cooperation of the Hellenic Police Headquarters,

1.4. the investigation of cases of suicide or disappearance, announced through the Internet,

1.5. providing assistance to the competent government agencies, to prevent suicides announced through the Internet.

To fulfill its mission, the Department of Administrative Support and Information Management, cooperates with the Division of Management and Analysis of Information, as defined in the provisions of the Article 22 of Law 4249/2014, to which it sends information collected by the Departments of the Division.

The Department of Administrative Support and Information Management serves as a contact point to the Council of Europe Convention on Cybercrime (Budapest Convention) and Directive 2013/40 / EU, on matters of attacks against information systems (Article 6 of Law 4411/2016).

2. The responsibilities of the *Department of Innovative Actions and Strategy* are the following:

2.1. the actualization of informative presentations for citizens and organizations on Internet and cybercrime issues, through the implementation of various actions, such as conferences, workshops and teleconferences, as well as the organization of other innovative actions in the field of combating cybercrime,

2.2. the development of strategic plans related to investigating cybercrime,

2.3. the promotion and publication of the social work of the Agency through the creation and management of profiles on social networking sites ("Twitter", "Facebook", etc.), exclusively for the purposes of communication, information and awareness of the citizens on issues related to the various threats and risks of cyberspace,

2.4. monitoring of all developments in cybercrime, both domestically and internationally, and preparing a relevant annual report with conclusions regarding these criminal activities committed in the country's territory, and submitting specific proposals to address the criminal issues, and

2.5. the recording and observance of criminal actions and the preparation of a statistics report related to cybercrime.

3. The *Department of Security of Electronic and Telephone Communications and Software and Copyright Protection* operates in accordance with the provisions of the Law 7001/2/1261-(21), common Ministerial decision. Additionally, this Department is responsible for:

3.1. handling criminal cases related to illegal penetration in computer systems and theft, destruction/alteration or illegal circulation of software, digital data and audiovisual works that take place throughout the country,

3.2. aiding other competent authorities that investigate these types of criminal cases, in accordance with the applicable law, and

3.3. the provision of the necessary technical assistance to the other Departments of the Agency, the conduct of digital and Internet research using modern technological equipment and the digital and Internet analysis of digital data, files and other media and findings, in cases of investigation of serious cases within their authority.

4. The duties of the *Department of Internet Protection of Minors* are the following:

4.1. the investigation and prosecution of crimes committed against minors using the Internet and other means of electronic or digital communication and storage,

4.2. investigating cases of cyber bullying of minors, and

4.3. to provide assistance to the competent state's authorities in investigating cases related to crimes described in subsections "4.1" and "4.2", for which specialized technical or digital investigation is required.

5. The responsibilities of the *Department of Investigation of Financial Crimes,* are as follows:

5.1. the investigation and prosecution, in cooperation with the Financial Police Division and the other competent national, European and foreign authorities, that investigate financial crimes and in particular cybercrimes which are either committed by using electronic means and new technologies, against the financial interests of the public and of the national economy in general, or possess the traits of organized financial crime and their investigation requires specific technical knowledge or experience, 5.2. the investigation of financial cybercrime, in cases where specialized technical or digital investigation is required,

5.3. providing assistance to government agencies in investigating cases involving virtual/digital currencies,

5.4. to provide assistance to the competent state's authorities, investigating cases related to crimes described in subsections "5.1" and "5.2", for which specialized technical or digital investigation is required.

6. The tasks of the *Department of Special Investigations and Digital Investigation*, are the following:

6.1. the handling of severe and organized crime cases, as well as all traditional crimes committed through the use of the Internet, the investigation of which can only be carried out through specialized technical or digital investigation, and is considered extremely difficult with the utilization of any other common police practices,

6.2. the inspection and investigation of the Internet and of any other means of electronic communication and digital storage, for the detection, tracing and prosecution of criminal actors, throughout the country,

6.3. to provide assistance to the competent state's authorities, which investigate cases mentioned in subsections "6.1" and "6.2", for which specialized technical or digital investigation is required.

For the fulfillment of its mission, the Hellenic Cyber Crime Division cooperates with all competent regional authorities of the Hellenic Police and in particular with the Division of Informatics, the Division of Management and Information Analysis, the Division of Economic Police and the Security Divisions of Attica and Thessaloniki. Moreover, in this context, the CCD cooperates with other competent authorities of the country, as well as with corresponding authorities and organizations of the EU and other foreign countries, in accordance with the applicable provisions and the relevant international agreements and conventions.

The CCD implements and utilizes all the necessary modern technical means and specialized equipment. The police staff is specifically trained to apply the utilized methods tools, as well as in all relevant and necessary practices, for the effective fulfillment of the Division's mission.

## 4.2 Interviews from police agents

From the author's point of view, it is critical to comprehend both the challenges faced by a LEA, specialized in cybercrime investigation, as well as how the entire theoretical analysis of cybercrime investigations is applied in practice. Therefore, the author has requested and granted the permission to interview high-ranking officers of the Hellenic Cyber Crime Subdivision of Northern Greece. For reasons of protection of personal data, no information that may possibly identify the interviewed police agents is included. In summary, the questions asked to the police agents of the CCU are related to a brief analysis of the investigated cybercrimes, the levels of cooperation between the Hellenic LEA and the various SMPs, as well as the international cooperation among all police agencies, worldwide. At the same time, the police officers were asked about their personal opinions on the subject of the responses they receive from various SMPs, both via legal processes and through the communication platforms, that each SMP has implemented. Finally, the interviewed police agents were invited to suggest certain proposals, that would improve the level of cooperation, between LEAs and SMPs.

### 4.2.1 Interview #1

**Question:** What is your police status and what is the subject of the Division you are the head of? Which are the relative criminal offences under investigation?

**Answer:** *I am a Police Director and I am the head of the Cyber Crime Subdivision of Northern Greece. Our police Agency investigates all kinds of cyber related criminal activities, such as online frauds, personal data breaches, child sexual abuse/exploitation, attacks on critical infrastructures and hacking. Apart from criminal investigation, our Agency interacts with the public in order to inform them regarding any imminent cyber threats and to receive complaints involving online criminal offences.*

**Question:** How and to what extent has cybercrime evolved in the past years?

**Answer:** *Unfortunately, cybercrime has evolved dramatically in the last few years.*

*Worldwide, all police agencies and other investigating organizations have reported numerous criminal activities related to cybercrime. The problem is that as the usage of the Internet, and especially social media, rises, more criminals tend to be active in cyberspace. The annual reports issued by both FBI and EUROPOL, which analyze all kinds of* *cybercrime, are very helpful in order to understand the increase of cybernetic criminal activity. The most worrying fact, is the increase of crimes related to child sexual abuse/exploitation, but also the increased tendency on personal data violations.*

**Question:** In your opinion, is the cooperation with the foreign companies to which Social Media Platforms belong to, deemed necessary? If so, how can this cooperation assist in eradicating cybercrime?

**Answer:** *Cooperation with foreign companies that own social media, can offer many advantages in the investigation processes of online criminality. In addition to cybercrime, foreign companies can also support the prosecution of the so-called traditional criminal activities. Of course, this cooperation must be based on the goodwill of both parties, in the fight against crime. The most important issue related to this collaboration is the fact that most social media establishments are based in the U.S.A. and therefore, the interaction with them becomes quite difficult. In any case, if this cooperation succeeds, it can eradicate crime in a great extent, as almost all criminals are active in some way on the Internet, either by attracting victims though it or by using it for personal use.*

**Question:** Does cooperation between your Division and the various foreign companies, that Social Media Platforms belong to, actually exist? If so, which are these foreign companies and what kind of data do you usually enquire for?

**Answer:** *Fortunately, most social media companies worldwide collaborate with all police agencies. Social media have either created personal platforms to disclose the requested data or provide information through international law enforcement authorities (e.g., EUROPOL). Usually, the companies we work with are "Facebook" / "Instagram", "Twitter", "Whatsupp" and "Google", which also have their own communication platforms. Of course, there are other companies, such as "PlanetRomeo" and "TikTok", which provide data through international police cooperation. The most commonly requested data are the electronic traces (IP addresses) of users and the data provided by the users during the creation of their account. In cases where we are searching for the current location of a missing person, we request for information regarding his/her geolocation activity.*

**Question:** Are you satisfied with the level of cooperation that these foreign companies provide? In your opinion, is there any way that this cooperation can change in order to facilitate an investigation's methods and practices?

**Answer:** *Certainly, the cooperation between our police Agency and the foreign companies that control social media is quite satisfactory. The only issue that arises is the time-consuming processes for providing the requested data, which in combination with the national legislation, may lead to the non-use of the disclosed electronic traces. Therefore, the faster satisfaction of our requests, is an issue that must be resolved immediately.*

**Question:** Do you believe that the mechanisms of international cooperation among countries have contributed to the cooperation of foreign Social Media Platforms?

**Answer:** *International cooperation mechanisms have been very helpful, especially in cases where the companies to which social media are owned by, have not yet implemented platforms for direct communication with the police authorities. Social Media Platforms that are based abroad and do not have such mechanisms, provide the requested data only through the channels of police cooperation between countries. At the same time, in addition to the EUROPOL and INTERPOL channels, there are several countries that have incorporated the so-called European Investigation Order, in which any European country can request information from foreign companies through the relevant Justice departments.*

### 4.2.2 Interview #2

**Question:** What is your police status and what is the subject of the Department you are the head of? Which are the relative criminal offences under investigation?

**Answer:** *I am a high-ranking officer of the Hellenic Police and I am the head of the Department of Security of Electronic & Telephone Communications and Protection of Software & Copyright of the Cybercrime Prosecution Subdivision of Northern Greece. The subject of the Department I am in charge of is related to the investigation of criminal offenses related to cases of illegal intrusion into computer-information systems, violation of the confidentiality of electronic communications, and theft, destruction or illegal circulation of software, hardware, digital data and audiovisual means. The criminal offenses that are basically related to these criminal cases are the crimes against telecommunications of the Penal Code (Articles: 292A "Crimes against the security of telephone communications", 292B "Obstruction of the operation of information systems", 292C, 292D*

*“Abuses of the public telecommunications “ and 292E “Obstruction of telecommunications”), the crimes of violation of individual privacy and communication of the Penal Code (Articles: 370B “Illegal access to information system or data”, 370C, 370D and 370E), and the crimes described by the provisions of Law 2121/1993 “on Intellectual Property” and P.D. 343/2002 “on the protection of subscription services”, without, excluding any confluence with other criminal offenses. Finally, the investigation of these criminal offenses is carried out through the collection of evidence and data from the Internet and digital investigation, and their analysis, with the ultimate goal of discovering and finally identifying the initially unknown or suspected perpetrators.*

**Question:** How and to what extent has cybercrime evolved in the past years?

**Answer:** *Cybercrime is the crime of the modern Information Age. As information, either in the form of processed data (software, audiovisual works, etc.) or organized data (databases, etc.), is stored in digital systems and they are interconnected on a large scale through networks and the Internet, genuine cybercrime thrives, as Information itself tends to be the object of crime. In addition, the high interconnection of information systems creates new fields of action for criminals who use new technologies and the Internet to commit traditional crimes (non-genuine cybercrime), in which the object of the crime is not the Information itself, but anything else apart from it. It is obvious, that every aspect of modern life includes new technologies, e.g. the Internet and information systems, and consequently cybercrime becomes an integral part of it with ever-increasing tendencies, to the extent that technology itself is also a part of it.*

**Question:** In your opinion, is the cooperation with the foreign companies to which Social Media Platforms belong to, deemed necessary? If so, how can this cooperation assist in eradicating cybercrime?

**Answer:** *Social networks could be described as the “new order of things” in our modern lives. Through them, the communication of hundreds of millions of people around the world is achieved, transactions are promoted in every possible way, a huge amount of information is exchanged, etc., while the average modern person maintains a digital face in a “parallel” virtual world. Consequently, the infringement of a person’s legally protected rights through social networks disrupts the legal order significantly and to a large extent, making the enforcing of penalties on criminal actors, crucial. In this light, cooperation with the companies that manage social networks is deemed necessary in order to enable the detection and prosecution of perpetrators of heinous acts committed by them,* *by maintaining and providing to the Law Enforcement Authorities the information that will lead to their identification, but also preventively by adopting practices and methods that will exclude the "activities" of the offenders on a case-by-case basis. If these collaborations generate the desired results, then they will be utilized as a preventative method for any ambitious perpetrators.*

**Question:** Does cooperation between your Department and the various foreign companies, that Social Media Platforms belong to, actually exist? If so, which are these foreign companies and what kind of data do you usually enquire for?

**Answer:** *Several foreign social media companies have developed specialized communication techniques, through which Law Enforcement Authorities can interact with them, in order to "fight" cybercrime. However, many of them require highly time-consuming legal procedures to provide the data, resulting in the loss of information that would be used for the investigation of crimes (e.g., mutual legal assistance treaty). On the other hand, there are companies that provide the requested information directly to our Agency, for legal use in court proceedings. Such companies are mainly "Facebook", "Instagram", "Google" (for "YouTube"), etc., while the requested data mostly concern Internet connection logs, i.e. IP addresses with their respective timestamps, as well as any other available identification and communication information of the user, such as registered identification details, telephone, email, payment information, and any other information stored by each company that can be used to continue the investigation, until the perpetrator of the crime is detected and identified.*

**Question:** Are you satisfied with the level of cooperation that these foreign companies provide? In your opinion, is there any way that this cooperation can change in order to facilitate an investigation's methods and practices?

**Answer:** *The level of cooperation will always have room for improvement. Of course, the foreign companies with which we cooperate, already provide enough information for the further investigation of cybercrime criminal cases. Usually, the obstacles in providing the requested information are of legal nature, according to the law that applies in each company. In particular, although foreign companies retain information useful and usable for the detection of perpetrators, they may not provide them to us, depending on the threatened legally protected right, such as the foreign companies "Facebook" and "Google" do not provide data in cases where the legally protected right, is the freedom of speech. From a technical point of view, improvement can be achieved by mandatory* *application of procedures for verifying the data provided by users, such as email addresses, telephone numbers, etc., so that the data recorded is as consistent, valid and accurate as possible, so they can be used as solid evidence to identify the perpetrators on a case-by-case basis. In addition, a significant improvement could be made in the time requirement for the provision of the requested data, i.e. "the faster, the better".*

**Question:** Do you believe that the mechanisms of international cooperation among countries have contributed to the cooperation of foreign Social Media Platforms?

**Answer:** *Judging by the procedures used to exchange information through international co-operation between countries (either police co-operation or judicial co-operation), the flow of information that can be used is in most cases hindered by legal issues, such as prohibitions on using this information for prosecution of the perpetrators, provided through international police cooperation, or by the time-consuming bureaucratic processes required in order to finally provide the information that will contribute to the investigation. In any case, the main issue is the time that elapses from the time of the request to the disclosure of the requested data, a fact that threatens the usability of the data provided in the end. Therefore, although international cooperation contributes to the detection of cybercrime, the issue that arises each time is of "time nature", regarding the utilization of the available data, thus mechanisms with faster response times would significantly improve the effectiveness of Law Enforcement Authorities. Comparing some of the mechanisms of international cooperation among countries, we can conclude that, for now, the process of the European Investigation Order is considered the most effective (with the limitation that this procedure includes cooperation only within the European Union), while in any case the direct communication and provision of data from the foreign companies on a case-by-case basis without the intervention of the state's mechanisms, excels, purely due to the directness of the communication and the relatively short time required for the provision of the requested data.*

### 4.2.3 Interview #3

**Question:** What is your police status and what is the subject of the Department you are the head of? Which are the relative criminal offences under investigation?

**Answer:** *I am a police lieutenant colonel and I currently serve as the head of the Department of Investigation of Financial Crimes. As the name of the department implies, the main responsibility of the department I supervise is the prosecution of economic crimes committed through the Internet, and online fraud is the one that we mostly meet nowadays.*

**Question:** How and to what extent has cybercrime evolved in the past years?

**Answer:** *It is a matter of fact that online crimes evolve day by day. During the last few years, we have often witnessed a rapid shift to the types of online criminality. For instance, if you recall the threat reports ENISA has produced since 2013, you will notice that the tactics, techniques and procedures (TTPs) the offenders use have changed scientifically. For example, despite malware remains a top threat for information systems, the evolution and proliferation of Internet enabled devices, have changed the way attackers act, meaning that they usually tend to attack less secure devices. Last but not least, the emergence of ransomware has significantly changed the information security landscape.*

**Question:** In your opinion, is the cooperation with the foreign companies to which Social Media Platforms belong to, deemed necessary? If so, how can this cooperation assist in eradicating cybercrime?

**Answer:** *In my point of view, close cooperation between law enforcement and industry is the key to minimize online criminality. Consider that private companies possess the information needed for law enforcement to act effectively. Law Enforcement Authorities across the globe require private sector to disclose information for investigation purposes. On top of that, consider that private industry including Social Media Platforms are responsible for applying security measures to harden their systems. Of course, cooperation with Law Enforcement Authorities could also benefit private sector in terms of applying best practices.*

**Question:** Does cooperation between your Department and the various foreign companies, that Social Media Platforms belong to, actually exist? If so, which are these foreign companies and what kind of data do you usually enquire for?

**Answer:** *Many private companies worldwide have acknowledged the benefits of close cooperation with Law Enforcement Authorities. So, they usually provide relevant information to my Agency when certain legal requirements are met. For example, "Facebook", "Google" and some other well-known companies usually provide information such as subscribers' registration details and connection history on a voluntary basis. Of* *course, there are companies that cannot provide direct information to foreign authorities due to restrictive legal frameworks in the countries they reside. In such cases, the Mutual Legal Assistance Treaties can be applied and local Law Enforcement Authorities can obtain the required information from those companies.*

**Question:** Are you satisfied with the level of cooperation that these foreign companies provide? In your opinion, is there any way that this cooperation can change in order to facilitate an investigation’s methods and practices?

**Answer:** *As stated above, some private sector companies provide information to my Agency on a voluntary basis. Even in these cases there is always room for improvement. To be more precise, it would be particularly important if we could minimize the timeframe between the inquiry and the provision of information.*

**Question:** Do you believe that the mechanisms of international cooperation among countries have contributed to the cooperation of foreign Social Media Platforms?

**Answer:** *I believe these mechanisms constantly mature. From the early stages of international cooperation, where the exchange of information was a complex procedure to the provision of information on a voluntary basis, that many companies support, a great improvement has been made. At this point I want to highlight the role that EUROPOL and INTERPOL have played to achieve such a success. Representatives of these organizations are in close cooperation with private sector, trying to improve the levels of international cybercrime investigation and, of course, tackle the illegal activities of organized crime groups acting on the Internet.*

### 4.2.4 Interview #4

**Question:** What is your police status and what is the subject of the Department you are the head of? Which are the relative criminal offences under investigation?

**Answer:** *I am a Police Major, and I have been the head of the Department of Internet Protection of Minors and Digital Investigation, of the Cyber Crime Subdivision of Northern Greece since 2015. The territorial jurisdiction of our Division extends to Northern Greece, Thrace and the Northern Aegean islands, whilst the responsibilities of the Department of Internet Protection of Minors and Digital Investigation, are the following:*

i. *the investigation and prosecution of crimes committed against minors using the Internet and other means of electronic or digital communication and storage,*

ii. *investigating cases of cyber bullying and racism or xenophobic content on the Internet, as well as cases involving suicide and cases of suicide or disappearance via the Internet,*

iii. *providing assistance to the competent state's authorities for the prevention of suicides announced via the Internet, as well as to the authorities investigating cases of crimes committed on the Internet in accordance with the applicable law.*

*In practice, the most serious cases, and the main object of the Department's staff, is the criminal investigation of offenses against sexual freedom, committed online against minors, such as violations of Articles 337 "Insult of sexual dignity," 348A "Child sexual abuse/exploitation", 348B "Attracting children for sexual reasons" and 348C "Pornographic performances of minors ", of the Hellenic Penal Code.*

**Question:** How and to what extent has cybercrime evolved in the past years?

**Answer:** *It is common knowledge that the use of the Internet, has not only increased dramatically in the past few years, but it is now an integral part of our lives, to the point that our life is considered unimaginable without its daily use. From transactions to entertainment and human interactions, the Internet is more or less used everywhere. In the age of globalization, the Internet is said to have provided an easy and cost-effective solution to issues related to communication, created by the ever-increasing physical distance. Today, the communication between two entities in opposite parts of the world not only does not seem impossible, but with the use of the Internet can be achieved without much cost and resources.*

*During the last year that the whole planet is plagued by the covid-19 virus and the distance in communications has become an inviolable rule for health reasons, Internet communication has replaced even the most traditional forms of live communication, such as education. The explosive increase in the use of the Internet for everyday purposes, has resulted in the rapid increase in the use of the Internet for illegal activities. The benefits and anonymity of the Internet are being exploited, not only by law-abiding citizens, but also by those who wish to commit a crime, as the physical distance from the victim gives them the feeling that they will not be located in order to face the consequences of the law.*

*As a result, it is more preferable from criminals to commit crimes online, rather than naturally, as in the past. Consequently, computer frauds, hacking of subscription services, sexual harassment and attraction of minors, circulation of child sexual abuse/exploitation, etc., are crimes that are committed mainly through the Internet.*

**Question:** In your opinion, is the cooperation with the foreign companies to which Social Media Platforms belong to, deemed necessary? If so, how can this cooperation assist in eradicating cybercrime?

**Answer:** *As mentioned above, the combination of technology and Internet use has eliminated the physical distances in communication. Thus, we can easily communicate with a friend who is a few meters away, using a social networking application provided by a company based in the United States of America and using servers in Ireland. However, the phenomenon of communications' globalization creates many complex problems for Law Enforcement Authorities, in cases of criminal investigation of crimes committed through the Internet.*

*Solving the problems that sometimes arise seems impossible, as the initiation and completion of the existing legal procedures (e.g. mutual legal assistance treaty) to obtain the required data from foreign companies requires a sufficient period of time, while this data is stored by national ISPs for a limited period of time, depending in each case on the applicable national law. For this reason, there is an urgent need for direct and close cooperation with foreign private companies that provide various Internet communication applications, in order to achieve a rapid criminal investigation of cybercrimes.*

**Question:** Does cooperation between your Department and the various foreign companies, that Social Media Platforms belong to, actually exist? If so, which are these foreign companies and what kind of data do you usually enquire for?

**Answer:** *Our Agency, like any other Law Enforcement Agency worldwide, has implemented direct communication channels with the major foreign companies that provide various online communication applications, such as "Facebook", "Google", "Twitter", "Microsoft", "Kik Interactive", etc. Thus, during the investigation of serious criminal cases, our Agency submits direct requests for the provision of the required data, which are usually electronic traces (log data) and all available registration and payment details (registration / payment details), accompanied with a relevant Prosecutor's/ Judicial Order. Then, the companies examine the submitted requests and if the legal conditions are met, they provide the requested data, directly to our Agency, in a relatively short period* *of time. In this way they provide immediate and substantial assistance in the prosecution of cybercrime, which in any other case, would have been extremely difficult.*

**Question:** Are you satisfied with the level of cooperation that these foreign companies provide? In your opinion, is there any way that this cooperation can change in order to facilitate an investigation 's methods and practices?

**Answer:** *The direct cooperation of our Agency with the companies that provide the various Internet communication applications, has numerous benefits on the investigation of crimes, and is considered as a valuable tool in the pre-investigation process. There is certainly room for improvement, such as the increase of the categories of data that these companies can provide or the reduction in response times. However, although there is a mutual determination to improve the already existing cooperation, the current legislation is often an obstacle for its improvement. For example, due to the General Data Protection Regulation (GDPR), it is not possible for Social Media Platforms to provide specific information, such as the content of a user's communication. Also, due to the constitutionally guaranteed freedom of speech in the U.S.A., it is not possible for Social Media Platforms to provide data related to criminal activities regarding slanderous comments, posted publicly by users.*

**Question:** Do you believe that the mechanisms of international cooperation among countries have contributed to the cooperation of foreign Social Media Platforms?

**Answer:** *In addition to the channels of direct communication with foreign companies, provided by the above-mentioned procedure, in the field of combating sexual abuse and exploitation of minors in general, which is the main object of my Department, there is another level of international cooperation, which is worth mentioning.*

*Based in the U.S.A., the National Center for Missing and Exploited Children (NCMEC) exists and operates, while the National Child Exploitation Coordination Center (NCECC) exists and operates in Canada. These organizations cooperate with various other organizations and national ISPs, in a joint effort to combat the phenomenon of the reproduction of child sexual abuse/exploitation and its circulation, through the Internet. When the aforementioned companies or organizations discover that child sexual abuse/exploitation material is being circulated through their information systems, they shall inform the competent authority, providing it with additional information about the users involved in this criminal activity. The latter forwards the provided information to the competent Law Enforcement Authorities. In case that the aforementioned criminal activity is detected by* *users within the Hellenic territory, a large amount of valuable information provided on a voluntary basis by the organizations and private social media companies, end up through the channels of international police cooperation (EUROPOL- INTERPOL), in our Agency, in order to assist the investigation of sexual exploitation of minors. A thorough investigation follows, which results in the identification of criminals and their arrest, a fact that without the above-mentioned procedure would have been completely impossible.*

In conclusion, as the high-ranking officers have stated in their interviews, cybercrime is evolving constantly. Although the enjoyment of SMPs' services is considered to be a necessity in our society, cybercriminals tend to exploit the provided benefits, in order to gain unlawful profit. Police agents, applying all sorts of traditional policing methodologies and technical practices, are trying their best to eradicate cybercrime. The cooperation amongst SMPs and all LEAs worldwide, has in a great extent supported this purpose. Additionally, the international cooperation amongst all LEAs is considered to be of outmost necessity, due to the physical and legal boundaries excluding non-U.S.A. police agencies from the immediate provision of the requested data. All in all, the police agents have clearly described that the biggest issue that rises from the existing cooperating procedures is the time-consuming processes regarding the disclosure of a user's data, which, combined with the long lasting legal and bureaucratic proceedings, may result in the extinction of the unknown criminals' trails. In the future, these problems ought to be resolved, as they detain the identification of the unidentified perpetrators and the elimination of online criminal activities, in general.

## 4.3 Real time scenarios

### 4.3.1 Intention to commit suicide

One of the most challenging types of investigations handled by a cybercrime agent are the incidents where users express their intention to commit suicide. In these cases, users usually upload a post on their personal account or communicate with others and confess their dark thoughts. The challenging part of this type of investigation is the identification of the unknown user in a limited amount of time. On most occasions, the investigations involving the identification and localization of the user in question are carried out by experienced police agents, who seek for details that will prevent the occurrence of the suicide. LEAs communicate with the SMP that the investigated person used to confine his/her intentions and request for the disclosure of the data that will immediately eliminate the possible threat and, eventually, save a person’s life. In this scenario, we will examine a case where a person directly contacted a virtual friend, using a SNS, and expressed his/her intention to commit suicide.

The CCU received an anonymous tip by a civilian, via its call complaint center, informing the Agency that an unknown user of a SNS had sent a direct message to another user of the platform, through which s/he had confessed his/her intention to commit suicide. The police officer who received the tip, requested the civilian who informed the Agency to provide further information regarding the incident, such as a screenshot of the user’s account and the exchanged messages, through which the unknown user voiced his/her suicidal intentions. The unknown informant sent the requested data to an experienced police agent, who then proceeded on evaluating the case.

After the assessment of the situation and its characterization as an “emergency”, the police agent who handled the case proceeded on sending an “emergency data request” to the SNS that the investigated person employed, in order to communicate with his/her virtual friend. Through the request, the law enforcer asked for the disclosure of data related to the user’s recent log data (IP addresses and timestamps), the information that the user in question provided to the SNS at the time of his/her registration and, most importantly, the current geolocation activity. Through its automated processes, the SNS enquired about the reasons that characterized the case as an “emergency” and solicited for detailed proof, in order to disclose the user’s data without the former provision of a signed legal proceeding. Without losing any time, the police officer responded with a brief explanation of the case, supplemented with attached screenshots of the messages. The SNS immediately provided the requested information to the LEA, apart from the geolocation data, as the investigated user had disabled the location feature of the SNS.

Once the handler of the case received the information s/he needed in order to identify the unknown user and locate his/her current whereabouts, s/he then proceeded on examining the data provided by the SNS. The first step was to analyze the log data, in order to match the provided IP addresses with their corresponding ISPs. Then, s/he proceeded on examining the registration data of the user, seeking for information that would probably identify him/her. As the latter method did not pay off, the police agent focused on the only traces s/he had; the log data of the investigated person.

Afterwards, the law enforcer contacted the corresponding ISPs, which resulted from the analysis of the log data (two different national ISPs) and requested for the disclosure of the identification information of their subscribers, to whom the IP addresses were assigned to. According to the first ISP's response, the requested IP addresses where public (i.e., NAT IP addresses) and were not assigned to any subscriber. The second ISP matched the requested IP addresses to a single subscriber and provided his/her identification details.

Thus, the investigation so far resulted in the disclosure of one (1) subscriber's identification details. After further examination of the subscriber's provided identification details and research through the LEA's databases, the police agent came up with a discovery. The subscriber had an adolescent child, whose photographs and identification details resembled those of the user who sent the suicidal messages. The police agent immediately contacted the local police department's officers, who in turn sent a police crew to the identified subscriber's residence, in order to determine if the adolescent was indeed the user who sent the messages and, in a positive case, to ensure his/her physical and mental integrity. The dispatched police officers located the citizen, verified that s/he was the actual user who expressed his/her intention to commit suicide, ensured his/her physical integrity and escorted him/her to the local police department. During the citizen's detention at the department, s/he was interviewed by a specialized phycologist in order to assess his/her mental integrity and determine how to further handle the situation. All in all, the investigation resulted in the identification of the unknown user and, at the end of the day, saved his/her life.

At this point, it must be clarified that under the applicable law, both the disclosure of a user's data from a SMP and the provision of a subscriber's identification information, require a former issue of a signed legal proceeding. In cases of imminent threats of life, due to the severeness of the situations, the police agents acquire for the immediate provision of the aforementioned data without a prior issue of such a proceeding, from both SMPs and national ISP, as they can be long lasting procedures, which may hold back the investigation and possibly result in the occurrence of the incident. In any case, after solving the case and rescuing the endangered citizen, the investigator who handled the case is obliged to inform the national legal authorities (e.g., district attorney, public prosecutor) in order to obtain the signed legal proceeding and then submit it to all the parties which provided the crucial information (i.e., SMPs and national ISPs.).

### 4.3.2 Personal Data – Identity Theft – Provoking minor to incest

Due to the implementation of the GDPR, identity theft and infringement of personal data are violations that are considered to be extremely severe and are being prosecuted accordingly. As most people have a registered account on numerous SNSs, the extraction of a user's personal data and his/her identify theft are considered to be a fairly easy process. It does not require any special skills or technical knowledge. Usually, these violations are committed with the purpose of executing other criminal acts. Perpetrators may "steal" any type of a user's personal data, in order to commit frauds, execute social engineering attacks or perform child exploitation activities. In order to emphasize the danger behind the commitment of such a criminal act, we will analyze a scenario, where the perpetrator "stole" a minor's identification details and photographs and used them to provoke another minor to incest.

An unknown criminal actor "stole" a minor's personal data (i.e., personal photographs name and surname), information that the minor had previously uploaded on his personal account on a SNS. Then, the perpetrator proceeded on creating another account, using the "stolen" data, on the same SNS. Soon after, s/he searched through the minor's "Friends" list and sent various messages to several of them, pretending to be the real user. One of them, also a minor, responded to the messages, as s/he thought s/he was communicating with his/her actual friend. The two users, criminal and victim, exchanged more than a few messages. The criminal's purpose was to gain the victim's trust and exploit him/her. Through his/her last message, the criminal actor attempted to provoke the minor to incest, by requesting the child to meet him/her and perform several sexual acts. The minor immediately informed his/her parents, who in turn filed a lawsuit against the unknown criminal actor.

As the case involved the theft of a user's personal data, it was handed over to the Department of Electronic and Telephone Communications Security and Software and Copyright Protection. Due to the severity of the criminal activity, it was assigned to an experienced police agent, who could handle both interviewing the victims and the investigation of the case. At first, the police officer questioned the minors/victims in order to acquire all the necessary evidence and proceed with the investigation. The victims provided the details of the criminal's account and screenshots with the exchanged messages. Thereafter, the police agent had to come up with a plan to make good use of the existing information.

Before heading into the heart of the investigation, the police agent ensured that s/he had in his/her possession all the legal paperwork demanded for the disclosure of the criminal's data. Then, s/he contacted the SNS, that the perpetrator exploited in order to communicate with the minor and requested for the disclosure of the account's processed information. Anything that the SNS could provide would be vital for the identification of the unknown criminal. Thankfully, the SNS provided the log data (IP addresses and timestamps), along with the information that the user provided at the time of his/her registration. As it turned out, the criminal used the data, "stolen" from the first victim, in order to register in the SNS and generate his/her account. Thus, the police agent was obliged to analyze the disclosed IP addreses, as they were the only evidence that could possibly result in the perpetrators identification.

The investigator analyzed the log data and matched the IP addresses with their corresponding ISPs. Later, s/he contacted the ISPs and requested for the disclosure of the identification details of their subscribers. Ultimately, the investigation so far provided the names of six (6) different people. One of them would probably be the unknown criminal.

As there was no other specialized investigation that the investigator could conduct to identify the perpetrator, s/he proceeded on interrogating the above-mentioned subscribers. Five (5) of them denied their involvement in the criminal act. However, the last subscriber admitted his/her close relation to the person who committed the investigated criminal activities. The agent demanded the interrogated subscriber to disclose the identity information of the suspect and conducted a brief search with the provided information, using the LEA's databases. As it turned out, the suspect had a history of criminal activities related to child sexual abuse/exploitation. Finally, a group of highly trained police officers searched for the suspect's current whereabouts and proceeded with his/her arrest and criminal prosecution.

### 4.3.3 Fraud

Fraud related cases are the most common criminal activities that occur in cyberspace. Crooks attract their victims in various ways, with the ultimate purpose of gaining unlawful profit. Regularly, they use SNSs in order to either upload the content that will probably result in the occurrence of the fraudulent activity or search for people who are considered to be too naïve to easily trust them. In this subsection, we will analyze the commitment of an illegal activity, where the criminal uses the SMP to upload his/her deceptive content and entice several victims.

The victim had searched for relevant advertisements on various SNSs, due to his/her interest in buying an agricultural machine (tractor). During his/her search, the user located an ad for the sale of a tractor which was posted by another user of the platform, in a private group. The victim contacted, via direct messaging, the alleged seller and after they agreed on the purchase of the tractor, they continued their communication both through the SNS's messaging feature and through conventional mobile interaction. After the settlement of the financial and shipment details of the transaction, the victim proceeded on depositing the money and waited for the delivery of the purchased machine. In the end, the victim realized the occurrence of the criminal activity, after the unknown perpetrator had received the deposited money, but never responded to his/her texts and phone calls.

At the time the victim realized that s/he was scammed by an unknown criminal, s/he filed a lawsuit against him/her and asked for the assistance of the CCU. The case was handed over to the specialized agents of the Department of Investigation of Financial Crimes. At first, the police officer assigned with the identification of the unknown perpetrator searched for information by utilizing traditional police practices. Specifically, s/he contacted the national telecommunication service provider and acquired for the information of the subscriber, who interacted with the victim. Moreover, he contacted the bank, through which the money was transferred, in order to acquire the data of the person who collected it. In both cases, the investigation did not result in the identification of the criminal. Nevertheless, the agent had another clue that s/he had not investigated up to that point. The criminal had a registered account on a SNS. Thus, s/he proceeded on requesting the criminal's account information from the related SNS.

After the issue of the required legal proceeding, the investigator contacted the SNS via its implemented request platform and requested for the disclosure of the information regarding the investigated account and shortly after, the SNS provided them. The investigator analyzed the provided log data (IP addresses and timestamps) and matched them with their corresponding ISPs. Hereupon, the police agent contacted the national ISPs and requested for the disclosure of the identification details of their subscribers. The investigation so far, resulted in the identification of three (3) different subscribers, who would possibly have a connection with the unknown perpetrator.

The police agent conducted a thorough search on the subscribers' identities through the CCU's databases and discovered that one of them was related to a prosecuted criminal, who committed several online frauds on various websites. The investigator contacted the local police department's officers, who handled that case, and asked for the provision of the investigation's details. The outcome of the local department's investigation was the prosecution of twenty-five (25) people, who formed a criminal organization and committed various frauds, either conventionally or online. The only evidence that was missing from the puzzle, was the correlation between the mastermind and the rest of the crew. As it turned out, the mastermind was the criminal who had created the account on the SNS and committed the criminal activity, investigated by the CCU. Subsequently, the last crook was arrested and prosecuted, along with the other members of the criminal organization.

### 4.3.4 Child sexual abuse/exploitation

Unlike all other relevant cybercrime investigations, the procedure of investigating a case involving child sexual abuse/exploitation is considered to be one of the most severe. The investigation of this category of criminal activity is usually handed over to high-ranking police agents, specialized in the field of combating criminal activities against minors. Usually, the high-ranking policemen do no act alone. They form a team of specially trained police officers, involving forensics specialists, psychologists and negotiators. CCUs investigate child sexual abuse/exploitation related cases that are committed by two different ways. The first case is when a user manages to acquire child sexual abuse/exploitation material from any possible online source, such as the dark web, and then distributes it to other users with the utilization of SMPs, free of charge or by payment. The second case is where a user communicates with a virtual friend, receives the heinous sexual material and then storages it for personal use. In this scenario we will examine the first case.

The Cyber Crime Division received an official report, via the EUROPOL channels, from the National Child Exploitation Coordination Center (NCECC) based in Canada, through which the organization provided several information involving the distribution and circulation of child sexual abuse/exploitation material. In its report the organization clarified that the material was distributed with the exploitation of a SNS. Additionally, the user who sent the material to other "netizens", was located within the Hellenic territory. Before heading in the thorough analysis of the scenario, it is essential to briefly analyze the operation of the NCECC.

The NCECC is an organization that collaborates with various SMPs and private companies, that provide any kind of Internet services, which are established in Canada, in a joint effort to eradicate the phenomenon of child sexual abuse/exploitation, circulated through the Internet. Whenever the aforementioned SMPs or companies realize that child sexual abuse/exploitation material is being distributed through their information systems, they shall inform the NCECC, providing the organization with additional information about the users involved in these criminal activities. The latter, in turn, not having the authority to investigate either the users or the criminal activities transmits the information provided to it, to the competent Law Enforcement Authorities.

As described, the NCECC provided the CCU with various information, regarding the log data that were assigned to the user who possessed and circulated child sexual abuse/exploitation material, by exploiting the SMP, along with other details that the above-mentioned user provided to the SNS at the time of his/her registration, such as a verified phone number, e-mail, username, etc. It is worth mentioning that the SNS, apart from the user's log data, also recorder the type of the device that the criminal actor regularly used, in order to access the platform. After the provision of the data, the Hellenic CCU proceeded on executing all the required legal proceedings in order to legally prosecute the criminal. Along with the execution of the necessary proceedings, the Police Agency analyzed the disclosed log data and matched the provided IP addresses with their corresponding ISPs. Later, the LEA contacted the corresponding national ISP, in order to identify the unknown user. After the provision of the identification details of the subscriber, the CCU handed over the investigation of the case to its Subdivision, as the user/criminal was located in the latter's territorial jurisdiction.

The high-ranking officer of the Department of Internet Protection of Minors, who was assigned with the further investigation of the case, put together a group of specialized and experienced police officers of the Agency and proceeded with the investigation of the criminal. The police officers conducted a thorough search of the person's criminal history and monitored his daily routine. Once they gathered all the necessary information, through espionage, the group of agents went to the criminal's known residence and conducted a lawful investigation at his/her house, in order to verify the existence of any type of physical or digital material, related to child sexual abuse/exploitation. At the time of the search, the police agents found and confiscated two (2) computers and one (1) cell phone, that belonged to the investigated subscriber. The first hint, that the police agents discovered and linked the investigated person with the criminal activity, was the fact that the confiscated mobile device, was the same type of device that the unknown perpetrator frequently used, in order to access the SMP.

In an on-site forensic examination of the confiscated computers, the forensic examinators did not find any material related to child sexual abuse/exploitation. Instead, by utilizing specialized methods and forensic tools, they discovered that the user of the confiscated devices, was the owner of the same e-mail account, that both NCECC and the SNS provided in their initial report, as the registered account of the criminal. Furthermore, the agents discovered that the user of the devices had created accounts on various cloud services, in order to upload and save his/her personal files online and not on any physical devices. Once the police agents gained access into the user's cloud accounts, they discovered that s/he had indeed uploaded several photos related to child sexual abuse/exploitation. Finally, the police officers wrapped up the investigation, gathered all the necessary evidence that verified the possession and distribution of child sexual abuse/exploitation material, arrested the criminal actor and prosecuted him/her for his/her atrocious actions.

# 5 Recommendations

## 5.1 Implementation of an International Intelligence Library

From what has been stated in the interviews which have been conducted with the high-ranking officers of the CCSNG, it is concluded that the long-lasting processes of providing a user's data can many times ruin the whole investigation. The author will hereby present his own proposal, in terms of international cooperation of entities involved in the field of tackling cybercrime. In case that these suggestions are applied and utilized properly, they may possibly minimize the risk of losing an ongoing investigation's evidence, along with preventing several types of cybercrime in general.

A common database, between SMPs and LEAs, should be developed. Through this database, authorized personnel of both entities could upload data of users who have been investigated, as well as prosecuted criminals. These data may either derive from the confiscated physical and digital devices of the perpetrators or from the reporting mechanisms of the SMPs. This database should be developed and handled by a third-party entity (private company or international organization), but in any case, the provision of the intelligence that would form the "International Intelligence Library" should be under the aforementioned entities' responsibility and meet all necessary EU data protection standards. With the implementation of this database, confiscated artifacts and intelligence gathered by LEAs would be uploaded, so that SMPs' either authorized personnel or automated processes, would be able to match them with their users' processed data and alert the police agencies, in case that the criminal actors utilized them in order to access the SMPs and perform any illegal activity. Likewise, SMPs could upload/import any data collected by its reporting mechanisms, so that in case a criminal activity occurred in the entity's virtual environment, the corresponding police authority, would immediately be informed in order to take all the appropriate legal actions, according to the criminal's networking data and the recorded geolocation activity.

To this extend, there are two important parameters which should be met as they are vital for the proper handling of the provided information. Initially, SMPs must deploy the proper mechanisms in order to verify a user’s data provided at the time of his/her registration, which lead to the generation of the uniquely identified profile. Specifically, whenever a user registers in any SMP and creates an account, the SMP must verify that at least some of the provided information are accurate. This process would not only reduce the number of fake accounts on SNSs, but it would also provide at least some reliable piece of information; so, the identification of the violator would be much easier in case of the infringement of the community’s rules. In any case, the SMPs must not exploit this process and request for irrational proportions of verified information. Nevertheless, the reasons behind the establishment of these virtual societies must not be neglected. Common people and average users employ SMPs in order to freely express themselves and share content. Not all “netizens” are criminals. That is the reason why the verification of a user’s data is a process that must be handled with caution and applied for specific categories of data, e.g. verified phone number, registered address or at least one verified user’s photograph.

On the other hand, LEAs which conduct criminal investigations and home searches in order to verify the commitment of a cybercrime, in general, and identify the unknown perpetrators, should perform specialized practices in order to preserve the confiscated artifacts. In detail, as it has been analyzed through the real time scenarios, whenever CCU’s agents handle a case which results in the identification and prosecution of the criminal actor, the artifacts utilized by the perpetrator during his/her execution of the criminal activity -either physical or digital means- are confiscated. Serial numbers of physical devices (e.g., laptops, mobile phones), accounts (e.g., e-mails, uniquely identified profiles on SNSs) and networking data (e.g., static IP addresses, MAC addresses, etc.) are the artifacts that are usually examined by LEAs and, therefore, used as evidence in the legal processes. Before the use of the impounded artifacts as evidence, specialized forensics experts should conduct a forensic examination on them and generate their “hash values” *(see above, p. 22)*.

The “hash values” ensure the data’s integrity. Subsequently, these “hash values” would be provided by the corresponding LEAs and uploaded on the “international library”, as intelligence for any future use. To this extend, whenever an official criminal investigator or a SMP’s authorized personnel uploaded any type of data to the intelligence library, they could easily be queried through the database and if the “hash values” matched with the provided information of any related criminal activity or corresponding criminal actor, then the investigators would have extra evidence either for the further investigation of the case or for the prosecution of the criminal actor.

Conclusively, this common database would create an international investigation platform, where both LEAs and SMPs could either provide or inquire any requested data and handle cases, in which either the unknown perpetrator or the investigated criminal activity went beyond their territorial jurisdiction. Time consuming proceedings would be eliminated, as already investigated cybercrimes' or identified criminals' information would be both uploaded in the database and available for any future use, for investigation and intelligence purposes.

## 5.2 The future of the Hellenic Cyber Crime Division

Apart from the recommended implementation of an "International Intelligence Library", the author will also present several proposals that match the CCD's vision and in case they are adopted, they may possibly ameliorate the future of the Agency.

Initially, the Agency should aim at establishing local cybercrime departments in every Local Police Division, which will be staffed either by local police officers, who are familiar with the community's needs and customs but need further training in the field of combating cybercrime or they will be recruited directly from the Police Academy with officers who possess the desired specialized knowledge and skills.

Furthermore, the LEA should furtherly cooperate with other regional state's authorities and assist them in cybercrime cases. Specifically, the LEA should seek in informing all public servants regarding the proper procedure of securing digital evidence, in cases of attacks on the critical infrastructures of the competent public authority in order to facilitate the further investigation of the cases. To this extend, the CCD should expand the already existing cooperation with other competent specialized authorities of the Hellenic Police for the dismantling of criminal organizations, which operate through the Internet.

In order to intensify its actions and preventive measures, as the CCD already investigates countless cybercrime cases, the Hellenic Police Headquarters should additionally consider recruiting in both the CCD and its CCSNG in order to efficiently continue to investigate the constantly evolving field of cybercrime.

Moreover, as the LEA handles several cases involving an individual's intention to commit suicide, the Agency should cooperate with non-governmental organizations and ISPs for the immediate disclosure of the networking data and the recent geolocation activity of the users who express suicidal intentions through the Internet.

An innovative recommendation would be the launch of the so-called *"cyber patrols"*. A *"cyber patrol"* is the inspection of the cyberspace by utilizing several tools and technical means, in order to detect the existence of hints that would possibly result in the commitment of a crime (distribution of drugs, frauds, terrorism, etc.). The gathered information would be properly evaluated and in cooperation with the other competent authorities, the CCD could initiate an investigation in order to verify the occurrence of the criminal activity.

The fact that the CCU's police agents need to be constantly well trained and specialized in fighting every type of cybercrime can easily be understood. Therefore, the CCD along with the Hellenic Police Headquarters should aim at educating its specialized agents through their participation in seminars, conferences and trainings initiated by national, European and international organizations. To this extend, the conduction of trainings to its staff, for the acquisition of theoretical and practical knowledge in the field of cyber security and specifically in the technical field of collecting and preserving digital evidence should be prioritized. Training and education in the field of combating cybercrimes which are committed through the exploitation of the "Dark Web" should be also emphasized.

Finally, the CCD should carry on with its engagement project, in terms of informing the citizens and raising public awareness on issues of preventing cybercrime. Hence, the Agency should maintain its course on hosting conferences and lectures to provide useful information and advice to the public and especially to young people, in order to protect them from any potential danger in cyberspace.

# Conclusions

Social Media Platforms have laid the foundations of the new "Information Era". Cyberspace is constantly expanding and these platforms have significantly contributed to this phenomenon. The establishment of cybernetic societies is depicted in every aspect of our everyday lives; "cybernauts" can communicate, transact, express their thoughts and worries, and ultimately turn their daily routine into a digital reality. Social media have existed for a while now, but their vast explosion was observed in 2005, soon after the introduction of Web 2.0. SNSs introduced numerous innovative services and technologies, which have utterly changed the nature of the Internet. Until then, users could only browse through websites, with the possibility of providing additional material or altering the existing content of the visited site being entirely absent. Hence, SMPs and in particular SNSs have established an imaginary relationship among all Internet operators. A single user can simply create an account and provide content that can be widely visible from every person on this planet. From "Facebook" and "Twitter, to "LinkedIn" and "Tinder", users can effortlessly find what they are searching for. Still, as SMPs depict the character of our society and contain every aspect of it, criminality could not be excluded.

Crooks and pedophiles, terrorists and hackers exploit SMPs' provided services to pester users in any possible way. Even though the benefits that these virtual communities provide are multilateral, the feature of anonymity can be a dangerous tool in the hands of an ambitious criminal. "Netizens" use the Internet in good faith and rarely understand that criminals have infiltrated its defenses. On several occasions, after the commitment of an online criminal activity, citizens have addressed the Law Enforcement Agencies in order to seek for protection and for further prosecution of the perpetrators. However, in many cases conventional police officers either lacked the proper specialized training or were simply unable to identify the unknown criminals, who were hiding behind the anonymity of the Internet. Thus, the introduction and formation of specialized police authorities, which would specifically investigate online criminal activities, was deemed critical. These police forces are widely known as Cyber Crime Units and since their establishment, they have contributed in a great extent to the protection of "netizens", the prevention of cybercrime and the identification of several unknown perpetrators. In any case, apart from the continuous specialized training and the endless effort that the cybercrime agents put in order to eradicate criminality on cyberspace, LEAs needed an ally in their fight against lawbreakers. These allies were no other than SMPs, the entities that have witnessed the thriving of criminality in their cores. All that these entities had to do was to simply provide information to LEAs which would in any other case be beyond their reach.

Whenever a user registers in a SNS and creates a new account, s/he is required to provide several personal information. E-mails accounts, usernames, telephone numbers, identification details, etc., are information requested by the user in order to generate his/her uniquely identified account. Moreover, as thoroughly analyzed in Chapter 2, SMPs gather and process a considerable amount of information, which the user voluntarily or unwillingly provides to the entity. Networking information, geolocation activity, affiliations, communications' content and many more are data collected through the platforms' automated processes and utilized to maximize the users' virtual experience. Nevertheless, as noble as data processing may appear to be, it is not always used for legitimate purposes. Distribution of an individual's stored information to third parties, unlawful process of data or infrastructure breaches, which caused the leaking of users' personal data, were merely some of the incidents that have taken place. Therefore, legislators were obliged to take the appropriate measures to eradicate these incidents and protect the users' personal data. The General Data Protection Regulation was put into force in order to reassure the public that by using any kind of SMP, it would not result in the infringement of the citizens' rights.

As mentioned above, SMPs collect and process all types of information from their users. As a result, LEAs were obliged to form an alliance with the entities, which in some way rule the "Information World" and seek their assistance in order to face the challenges of cybercrime investigations. Therefore, along with the implementation of international collaboration amongst all LEAs, Cyber Crime Units have cooperated with several SMPs in a joint force against cybercrime. Numerous SMPs have developed and implemented their own private platforms, through which police agents can request the disclosure of an unknown perpetrator's processed information. Furthermore, LEAs may request the provision of common users' data in cases of imminent threats of physical injury, suicide or missing person cases. All in all, SMPs are able to provide information, which in case they were examined and analyzed by an experienced and well-trained police officer, they would be able to solve any type of both online and traditional criminal activity.

Apart from the disclosure of a user's personal data, SMPs provide much more information to LEAs. Police agents utilize SMPs in order to engage the public, investigate perpetrators and perform intelligence techniques online. Engagement is of outmost necessity in any aspect of police work, as through this process LEAs can easily interact with the public, inform citizens regarding any ongoing criminal activity and prevent its spreading. Moreover, LEAs can receive tips from anyone who wishes to aid the police Agency, information that in many cases can either prevent the execution of a crime or save another person's life. Investigation and intelligence gathering are applied through several specialized methods and tools, like "O.S.INT.", "Social Media Profiling" and "Social Cyber Forensics". The aforementioned techniques can extract data from users' accounts, which if analyzed appropriately, they can possibly lead to the eradication of all kind of criminality, either online or in the real world.

A unique example of a Cyber Crime Unit that has utilized SMPs to eliminate cybercrime is the Hellenic paradigm. The Hellenic Cyber Crime Division is a LEA which except for solving numerous cases and identifying several unknown perpetrators, displays the authority's social aspect on a daily basis. The Agency has adopted most of the practices offered through the utilization of social media. Apart from developing its own websites, the LEA has created accounts on various SMPs in order to be a part of the existing virtual community. In addition, the CCD organizes plenty of seminars through which citizens and organizations can be well informed and protected against cybercrime and the cyberspace, in general.

Moreover, both through the real time scenarios and the conducted interviews with the high-ranking officers of the Agency, it can easily be assumed that an investigation revolving the identification of an unknown online perpetrator is not as easy as it is considered to be. The Agency consists of police officers with specialized training in every aspect of cybercrime. From forensics examiners to data analysts, ethical hackers and psychologists, the LEA tries to predict every imminent threat and its ultimate purpose is to prevent cybercrime before its occurrence. In case that the criminal activity has actually been committed, specialized police officers employ their knowledge and techniques and with the assistance of the SMPs they can methodically investigate the cybercrime and prosecute the identified perpetrator. The only issue that arises from the alliance forged among the Hellenic CCU and the various SMPs it that the disclosure of the requested data usually demands long-lasting procedures and time-consuming bureaucratic paperwork. In combination to the current legislation, according to which the national ISPs are obliged to delete subscribers' information after one year of storage, these two facts may possibly result in the loss of evidence that would probably identify an unknown criminal actor. Unfortunately, this is a challenge that regardless of technical training and specialization, no cybercrime agent can overcome.

Through the entire thesis, the concepts of users, cybercriminals, SMPs and CCUs have been thoroughly analyzed. One may easily come to the conclusion that these four entities consist the greatest part of the whole cyberspace. Users are the ones who enrich it with their content. SMPs are the bodies which unite the users. Cybercriminals exploit both of them to their own benefit. Last but not least, CCUs exist in order to protect both users and SMPs, and hunt down cybercriminals. So far, SMPs and CCUs have been cooperating in the digital war against cybercriminals. In case that this cooperation persists and continuously evolves, then it will eliminate cybercrime once and for all. But, if not? Hopefully, this is a question that we will never have to answer.

# Discussions

One of the issues raised regarding the disclosure and utilization of a user's personal data for legal investigations is the protection of an individual's right to privacy, which is specifically described in the Universal Declaration of Human Rights (UDHR). The right to privacy, is a fundamental right and is enshrined in Article 12 of the UDHR. According to it, *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*. Apart from the UDHR, it is also enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). In brief, both Articles protect all people against any unlawful and *"arbitrary interference"* with an individual's privacy, affiliations, personality, beliefs and communication. In respect to an individual's private life, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, titled "Respect for private and family life" and "Protection of personal data" respectively, mandate the protection of a person's personal information, of any kind, and his/her right to live without the externalization of its aspects. All the rights mentioned above were recognized in order to protect a civilian from both illegitimate and unlimited process or exploitation of his/her personal data.

On many occasions, both average users and offenders accentuate that LEAs trespass their right to privacy and acquire their personal data for various illegitimate reasons. They believe that due to their fundamental rights for privacy, by using SMPs and in particular SNSs, they build defensive walls against any case of data processing. Truly, these rights do protect data subjects and their privacy. Nonetheless, no one can claim that by using cyberspace, s/he can demonstrate his/her illegitimate purposes and not held accountable for them. Everyone must understand that by utilizing SMPs they just gain anonymity, not remission for their illegal actions.

The aforementioned rights were recognized in order to protect people from the phenomenon of arbitrary and unrestricted distribution of an individual's personal data to third parties. No one can abuse the legislators' good intentions which are no other than protecting the society's citizens. However, according to the common opinion, these fundamental rights were established in order to create imaginary legal boundaries, so that no law enforcer would be allowed to investigate anyone. To this extend, a criminal's right to privacy and right for protection of personal data would excess the rest of the peoples' rights to live peacefully, without any kind of intrusion.

Corresponding to Article 12 of the UDHR, Article 29 of the Declaration states that: *"In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."* While the UDHR's function is not the explanation of the Article by default, it assumes that limitations on a person's rights are desirable, albeit on some occasions necessary. A closer look to the definition of the term "crime" will clarify any raised confusion. When a person commits any type of felony, s/he infringes another person's fundamental rights. Either when it comes to the right to protection of personal data (Article 8, EU Charter of Fundamental Rights) or to the right to property (Article 17, EU Charter of Fundamental Rights), no one should be allowed to infringe them and take advantage of the legislators' protective wills. Thus, in cases that a person commits a crime, his/her right to privacy is thereby limited and the disclosure of his/her personal data, private life and any other type of information that could possibly identify the unknown perpetrator is not only considered legitimate, but most importantly it is deemed mandatory. After all, according to recital 7 LED *"Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation"*.

# Bibliography

[1] D. Miller, E. Costa, N. Haynes, T. McDonald, R. Nicolescu, J. Sinanan, J. Spyer, S. Venkatraman and X. Wang, "How the world changed Social Media.", 2016.

[2] Merriam-Webster.com Dictionary, Merriam-Webster, "Social media," [Online]. Available: https://www.merriam-webster.com/dictionary/social%20media.

[3] J. Brunty and K. Helenek, "Social Media Investigation for Law Enforcement.", 2012.

[4] D. M. Boyd and N. B. Ellison, "Social Network Sites : Definition, History, and Scholarship.", 2007.

[5] Merriam-Webster.com Dictionary, Merriam-Webster, "Netizen," [Online]. Available: https://www.merriam-webster.com/dictionary/netizen.

[6] Merriam-Webster.com Dictionary, Merriam-Webster, "Cybernaut," [Online]. Available: https://www.merriam-webster.com/dictionary/cybernaut.

[7] O' Reilly Media, Inc., "What is Web 2.0.", 2009.

[8] L. Mitrou, M. Kandias, V. Stavrou and D. Gritzalis, "Social Media profiling: a panopticon or omniopticon tool?", 2014.

[9] Wikipedia, "Wikipedia: About.," [Online]. Available: https://en.wikipedia.org/wiki/Wikipedia:About .

[10] Wikipedia, "When may we share your information?," [Online]. Available: https://foundation.wikimedia.org/wiki/Privacy_policy#when-we-may-share.

[11] M. Cross, "Social Media Security.", 2014.

[12] Y. Hu, L. Manikonda and S. Kambhampati, "What we Instagram: A first analysis of Instagram photo content and user types.", 2014..

[13] Twitter Inc., "How to access your Twitter data.," [Online]. Available: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data .

[14] Z. Zhang, "Infrastructuralization of Tik Tok: transformation, power relationships, and platformization of video entertainment in China.", 2020.

[15] WordReference.com | Online Language Dictionaries, "Sitting Ducks," [Online]. Available: https://www.wordreference.com/definition/sitting%20ducks.

[16] United Nations Office on Drugs and Crime, "Comprehensive study on cybercrime", 2013.

[17] United Nations, "UN Manual on the prevention and control of computer related crime", 1994.

[18] Council of Europe, "Convention on Cybercrime", 2001.

[19] Council of Europe, "Explanatory Report to the Convention on Cybercrime", 2001.

[20] EUROPOL - EC3, "Internet Organised Crime Threat Assesment (IOCTA)", 2019.

[21] C. Wilson, "Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and police issues for congress.", Updated 2008.

[22] ISO/IEC JTC 1, BS ISO/IEC 2382-1:1993. "Information technology. Vocabulary. Fundamental terms", 1994.

[23] INTERPOL, "Cybercrime operations.," [Online]. Available: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations.

[24] INTERPOL, "Cyber capabilities development.," [Online]. Available: https://www.interpol.int/Crimes/Cybercrime/Cyber-capabilities-development .

[25] EUROPOL, "EUROPEAN CYBERCRIME CENTRE - EC3. Combating crime in a digital age.," [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 .

[26] Federal Bureau of Investgation - F.B.I., "What we investigate?," [Online]. Available: https://www.fbi.gov/investigate/cyber.

[27] European Union Agency for Cybersecurity - ENISA, "A trusted and cyber secure Europe - ENISA", 2020.

[28] A. Rashid, H. Chivers, G. Danezis, E. Lupu and A. Martin, "Cybok: The Cyber Security Body of Knowledge.", 2019.

[29] D. Gašpar, "NoSQL Databases as Social Networks storage systems.", 2017.

[30] S. Lohr, "The Origins of 'Big Data': An Etymological Detective Story," 2013. [Online]. Available: https://bits.blogs.nytimes.com/2013/02/01/the-origins-of-big-data-an-etymological-detective-story/ .

[31] M. Smith, C. Szongott, B. Henne and G. Von Voigt, "Big Data privacy in public social media.", 2012 6th IEEE International Conference on Digital Ecosystms and Technolgies (DEST), 20.

[32] X. Wu, X. Zhu, G. Wu and W. Ding, "Data mining with big data.", in IEEE Transactions on Knowledge and Data Engineering, 2014.

[33] S. Sreeja and A. Sangeetha, "No science no humans, no new technologies no changes: Big Data a Great Revolution.", International Journal of Computer Science and Information Technologies, 2015.

[34] E. Wilder-James, "What is big-data? An introduction to the big data landscape.," [Online]. Available: https://www.oreilly.com/radar/what-is-big-data/.

[35] P. Warden, "Big Data Glossary.", 2011.

[36] European Union Agency for Cybersecurity - ENISA, "Cloud and Big Data - Big Data.," [Online]. Available: https://www.enisa.europa.eu/topics/cloud-and-big-data/big-data .

[37] M. T. Thai, W. Wu and H. Xiong, "Big Data in complex and Social Networks.", 2017.

[38] D. Ford, L. Florentina, I. Popovici, M. Stokely, V.-a. Truong, L. Barroso, C. Grimes and S. Quinlan, "Google Inc, Availability in globally Distributed Storage Systems", 2010.

[39] D. Tran, "Data Storage for Social Networks: A socially aware approach.", 2012.

[40] N. Ruflin, B. Helmar and S. Rizzoti, "Social data storage systems.", 2011.

[41] Neo 4j Inc., "What is Neo4j?," [Online]. Available: https://neo4j.com/.

[42] Microsoft, "Ensuring Data Integrity with Hash Codes," [Online]. Available: https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes.

[43] Twitter Inc., "Manhattan, our real-time, multi-tenant distributed database for Twitter scale," 2014. [Online]. Available: https://blog.twitter.com/engineering/en_us/a/2014/manhattan-our-real-time-multi-tenant-distributed-database-for-twitter-scale.html.

[44] Twitter Inc., "Hadoop filesystem at Twitter," 2015. [Online]. Available: https://blog.twitter.com/engineering/en_us/a/2015/hadoop-filesystem-at-twitter.html.

[45] MySQL AB, "MySQL Customer: Facebook.," [Online]. Available: https://www.mysql.com/fr/customers/view/?id=757 .

[46] R. Shroff and Z. Fong, "HydraBase – The evolution of HBase@Facebook," 2014. [Online]. Available: https://engineering.fb.com/core-data/hydrabase-the-evolution-of-hbase-facebook/.

[47] X. Li and T. Georgiou, "Migrating Messenger storage to optimize performance," 2018. [Online]. Available: https://engineering.fb.com/2018/06/26/core-data/migrating-messenger-storage-to-optimize-performance/.

[48] "Facebook Database [Updated] – A Thorough Insight Into The Databases Used @Facebook," [Online]. Available: https://www.8bitmen.com/what-database-does-facebook-use-a-1000-feet-deep-dive/.

[49] Google LLC., "Overview of Cloud Bigtable," [Online]. Available: https://cloud.google.com/bigtable/docs/overview.

[50] Google LLC., "About Google Data Centers," [Online]. Available: https://www.google.com/about/datacenters/.

[51] Facebook Inc., "Data Policy," [Online]. Available: https://www.facebook.com/privacy/explanation.

[52] Twitter Inc., "Twitters Privacy Policy," 2020.

[53] Tinder, MTCH Technology Services Limited, "Privacy Policy," [Online]. Available: https://policies.tinder.com/privacy/intl/en#information-we-collect .

[54] Reddit Inc., "Reddit Privacy Policy," [Online]. Available: https://www.redditinc.com/policies/privacy-policy-october-15-2020.

[55] European Union - European Data Protection Suprevisor, "The History of the General Data Protection Regulation," [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[56] OpenAIRE, "Guides for Researchers.," [Online]. Available: https://www.openaire.eu/sensitive-data-guide .

[57] C. Tikkinen-Piri, A. Rohunen and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review."", 2018.

[58] A. Kotsios, M. Magnani, L. Rossi, I. Shklovski and D. Vegak, "An analysis of the Consequences of the General Data Protection Regulation on Social Network Research.", 2019.

[59] Privacy Team, IT Governance, "EU General Data Protection Regulation (GDPR): An implementation and compliance guide.", 2016.

[60] G. Misra and J. M. Such, "How socially aware are Social Media privacy controls?", 2016.

[61] Information Commissioner's Office, "What is the right to rectification?," [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/#ib1.

[62] GDPRhub, "Article 22 GDPR," [Online]. Available: https://gdprhub.eu/Article_22_GDPR .

[63] B. Lord, "An Important Message About Yahoo User Security," [Online]. Available: https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security.

[64] R. Hackett, "LinkedIn Lost 167 Million Account Credentials in Data Breach," 2016. [Online]. Available: https://fortune.com/2016/05/18/linkedin-data-breach-email-password/.

[65] European Union Agency for Cybersecurity (ENISA), "Pseudonymisation techniques and best practises.", 2019.

[66] Kapersky Lab, "What is Data Encryption?," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/encryption.

[67] N. Goyal, K. Nekritz and S. Iyengar, "Building Facebook's service encryption infastructure.," [Online]. Available: https://engineering.fb.com/2019/05/29/security/service-encryption/.

[68] Australian Government. Office of the Australian Information Commissioner., "What is a privacy policy?," [Online]. Available: https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy/.

[69] Tumblr, Inc., "Privacy Policy".

[70] J. Mohan, M. Wasserman and V. Chidambaram, "Analyzing GDPR Compliance through the lens of privacy policy.", Vols. "Heterogeneous Data Management, Polystores, and Analytics for Healthcare.", 2019.

[71] EU/COE, "Joint project on regional cooperation against Cybercrime.", 2011.

[72] E. Martelozzo and E. A. Jane, "Cybercrime and its victims.", 2017.

[73] P. S. Bayerl, K. Horton, G. Jacobs and B. Akhgar, "Who wants police on social media?", vol. "Proceedings of the European Conference on Social Media (ECSM).", 2014.

[74] N. J. Keane, "Police use of Social Media to support community engagement - Its rise in Police practice in the UK. European Law Enforcement Research Bulletin.", 2016.

[75] National Policing Improvement Agency (NPIA);, "Engage: Digital and Social Media engagement for the police services.", 2010.

[76] T. R. Soomro and M. Hussain, "Social Media-Related Cybercrimes and techniques for their prevention.", 2019.

[77] The Police Foundation;, "The briefing: Police use of social media.", 2014.

[78] Merriam-Webster.com Dictionary, Merriam-Webster, "Cold case," [Online]. Available: https://www.merriam-webster.com/dictionary/cold%20case.

[79] IC3 - Cyber Division Federal Bureau of Investigation, "Internet Crime Report", 2019.

[80] EUROPOL - EC3, "Internet Organized Crime Threat Assessment (IOCTA)", 2020.

[81] "Twitter Investigation Report," 2020. [Online]. Available: https://www.dfs.ny.gov/Twitter_Report.

[82] Twitter Inc., "An update on our security incident.," 2020. [Online]. Available: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

[83] N. Ayres and L. A. Maglaras, "Cyberterrorism targeting the general public through Social Media.", 2016.

[84] A. Parlakkilic, "Cyber Terrorism through Social Media: A categorical based preventetive approach.", 2019.

[85] United Nations Office on Drugs and Crime;, "The use of the internet for terrorist purposes.", 2012.

[86] National centre against bullying, "Definition of bullying.," [Online]. Available: https://www.ncab.org.au/bullying-advice/bullying-for-parents/definition-of-bullying/ .

[87] C. E. Notar, S. Padgett and J. Roden , "Cyberbullying: Resources for intervention and prevention.", 2013.

[88] Cyberbullying Research Center., [Online]. Available: https://cyberbullying.org/.

[89] National Bullying Helpline, "What is Cyberbullying?," [Online]. Available: https://www.nationalbullyinghelpline.co.uk/cyberbullying.html.

[90] Facebook Inc., "Bullying Prevention Hub," [Online]. Available: https://www.facebook.com/safety/bullying/.

[91] R. D' Ovidio and J. Doyle, "A study on cyberstalking: Understanding investigative.", FBI L. Enforcement Bull, 2003.

[92] S. Hinduja, "Cyberstalking.," [Online]. Available: https://cyberbullying.org/cyberstalking.

[93] European Union Agency for Cybersecurity - ENISA, "What is "Social Engineering"?," [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering.

[94] Merriam-Webster.com Dictionary, Merriam-Webster, "Scammer," [Online]. Available: https://www.merriam-webster.com/dictionary/scammer.

[95] European Union Agency for Cybersecurity - ENISA, "Phishing-Spear Phishing.," [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing.

[96] European Union Agency for Cybersecurity - ENISA, "Malware.," [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware.

[97] NordVPN, "The top 10 most destructive viruses of all time.," 2020. [Online]. Available: https://nordvpn.com/blog/worst-computer-viruses/.

[98] Merriam-Webster.com Dictionary, Merriam-Webster, "Keylogger," [Online]. Available: https://www.merriam-webster.com/dictionary/keylogger.

[99] U.S. Securities and Exchange Commission., "Internet and Social Media Fraud.," [Online]. Available: https://www.investor.gov/protect-your-investments/fraud/types-fraud/internet-and-social-media-fraud#Social-media .

[100] Federal Bureau of Investigation - F.B.I., "Romance Scams.," [Online]. Available: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams.

[101] National Fraud & Cyber Crime Reporting Center., "Inheritance Fraud.," [Online]. Available: https://www.actionfraud.police.uk/a-z-of-fraud/inheritance-fraud.

[102] Merriam-Webster.com Dictionary, Merriam-Webster, "Sexting," [Online]. Available: https://www.merriam-webster.com/dictionary/sexting.

[103] Legal Information Institute, "Subpoena," [Online]. Available: https://www.law.cornell.edu/wex/subpoena.

[104] Twitter Inc., "Guidelines for Law Enforcement.," [Online]. Available: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support .

[105] Facebook Inc., "Information for law enforcement authorities.," [Online]. Available: https://www.facebook.com/safety/groups/law/guidelines/.

[106] North Carolina State University, "Subpoenas, Court Orders and Search Warrants," [Online]. Available: https://generalcounsel.ncsu.edu/legal-topics/lawsuits-and-litigation/subpoenas-court-orders-and-search-warrants/.

[107] Pinterest Inc., "Law enforcement guidelines.," [Online]. Available: https://help.pinterest.com/en/article/law-enforcement-guidelines .

[108] Legal Information Institute, "Search Warrant," [Online]. Available: https://www.law.cornell.edu/wex/search_warrant.

[109] Legal Information Institute, "Fourth Amendment," [Online]. Available: https://www.law.cornell.edu/wex/fourth_amendment.

[110] A. Abdalla and S. Y. Yavilgan, "Social Computing and Social Media. Chapter A: Review of Using Online Social Networks for Investigative Activities.", 2014.

[111] J. Goldbeck, "Introduction to Social Media Investigation, A Hands-on Approach.", 2015.

[112] O. Lynskey, *“Criminal justice profiling and EU data protection law: precarious protection from predictive policing,”,* International Journal of Law in Context, 2019.

[113] J. R. G. Evangelista, R. J. Sassi, M. Romero and D. Napolitano, "Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence.", 2020.

[114] Central Intelligence Agency - C.I.A., "INTelligence: Open Source Intelligence," [Online]. Available: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

[115] D. Trottier, "Open source intelligence, social media and law enforcement: Visions, contraints and critiques.", 2015.

[116] A. Bielska, N. R. Kurz, Y. Baumgartner and V. Benetis, "Open Souce Intelligence Tools and Recources Handbook.", 2020.

[117] "Intelligence Organizations - Mass Communication Interception and Analysis Solutions for Intelligence Organizations.," [Online]. Available: https://www.e-insight.gr/index.php/en/our-offerings-en/security-solutions/intelligence-organizations .

[118] R. N. Kocsis, "Criminal Profiling, Principles and Practice.", 2006.

[119] R. Yepes, "The art of Profiling in a Digital World.," 2016. [Online]. Available: https://www.policechiefmagazine.org/the-art-of-profiling-in-a-digital-world/.

[120] E. Casey, "Cyberpatterns: Criminal Behavior on the Internet.", 2012.

[121] WordSense.eu, "Cybertrail," [Online]. Available: https://www.wordsense.eu/cybertrail/.

[122] Merriam-Webster.com Dictionary, Merriam-Webster, "Modus operandi," [Online]. Available: https://www.merriam-webster.com/dictionary/modus%20operandi.

[123] N. Garcia, "The use of criminal profiling in a cybercrime investigation.", 2018.

[124] D. Povar and V. Bhadram, "Forensic data carving, in Digital Forensica and Cyber Crime.", 2010.

[125] A. Prasad and J. Pandey, "Digital Forensics.", 2016.

[126] T. Özyer, S. Bakshi and R. Alhaji, "Social Networks and Surveillance for Society.", 2018.

[127] S. Al-khateeb and N. Agarwal, "Deviance in Social Media and Social Cyber Forensics. Uncovering Hidden Relations Using Open Source Information", 2019.

[128] V. Khera, "Utilize Open Source Intelligence (OSINT) techniques to support digital forensics investigations.," 2020. [Online]. Available: https://cybersecurity-magazine.com/utilize-open-source-intelligence-osint-techniques-to-support-digital-forensics-investigations/.

[129] Hellenic Police - Cyber Crime Division., ""Activity Report, Cyber Crime Division, year 2019."," 2020.

[130] Hellenic Police - Cyber Crime Division., "CyberAlert," [Online]. Available: https://cyberalert.gr/en/.

[131] Hellenic Police - Cyber Crime Division., "Cyberkid," [Online]. Available: https://www.cyberkid.gov.gr.

# Appendix

## 1. Abbreviations

| | |
|---|---|
| SMP | Social Media Platform |
| U.S.A. | United States of America |
| LEA | Law Enforcement Authority |
| CCU | Cyber Crime Unit |
| Malware | Malicious Software |
| SNS | Social Networking Site |
| WWW | World Wide Web |
| DB | database |
| CV | Curriculum Vitae |
| iOS | i-Phone Operating System |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| ISO | International Organization for Standardization |
| ICT | Information Communication Technology |
| INTERPOL | International Police |
| CERTs | Computer Emergency Response Teams |
| EUROPOL | European Police |
| J-CAT | Joint Cybercrime Action Taskforce |
| IOCTA | Internet Organized Crime Threat Assessment |
| FBI | Federal Bureau of Investigation |
| IC3 | Internet Crime Complaint Center |
| ENISA | European Union Agency for Data Security |
| EU | European Union |
| GDPR | General Data Protection Regulation |

| | |
|---|---|
| PC | Personal Computer |
| NAS | Network-Attached Storage |
| HDFS | Hadoop Distributed File System |
| App | Application |
| HBASE | Hadoop Database |
| S3 | Amazon Simple Storage Service |
| EC2 | Amazon Elastic Compute Cloud |
| NLP | Natural Language Processing |
| NLTK | Natural Language Toolkit |
| WEKA | Waikato Environment for Knowledge Analysis |
| Graphviz | Graph Visualization Software |
| DSS | Distributed Storage System |
| JSON | JavaScript Object Notation |
| BSON | Binary JavaScript Object Notation |
| URL | Unified Resource Locator |
| Geolocation | Geographic Location |
| TFEU | Treaty on the Functioning of the European Union |
| DPO | Data Protection Officer |
| ECHR | European Convention on Human Rights |
| LED | Law Enforcement Directive |
| RNG | Random number generator |
| BTC | Bitcoin |
| UNODC | United Nations Office on Drugs and Crime |
| DDos | Distributed Denial of services |
| U.K. | United Kingdom |
| U.S.C. | United States Code |
| OSINT | Open-Source INTelligence |
| SCF | Social Cyber Forensics |

| | |
|---|---|
| API | Application Programming Interface |
| Wi-Fi | Wireless Fidelity |
| WTC | Web Tracker Code |
| CCD | Cyber Crime Division |
| CCSNG | Cyber Crime Subdivision of Northern Greece |
| CEPOL | European Union Agency for Law Enforcement Training |
| GAAD | Global Airport Action Days |
| EMMAV | European Money Mule Action |
| EBF | European Banking Federation |
| SIRENE | Supplementary Information Request at the National Entries |
| EUIRU | Europol 's European Union Internet Referral Unit |
| NCMEC | National Center for Missing and Exploited Children |
| NCECC | National Child Exploitation Coordination Center |
| MAC | Media Access Control |
| UDHR | Universal Declaration of Human Rights |
| ICCPR | International Covenant on Civil and Political Rights |

# 2. Image Sources

# 3. Legislation

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
2. Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018
3. 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
4. Charter of Fundamental Rights of the European Union, 26.10.2012, 2012/C 326/02
5. Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012
6. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5

7. Law 4624/2019 Government Gazette A’ 137/29.8.2019
8. Law 2472/1997, Governmental Gazette 50/A/10-04-1997
9. United States Code, 2006 Edition
10. Document 22003A0719(02), Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003
11. Code of Federal Regulations (CFR), Title 22. Foreign Relations, 92.54. “Letters rogatory” defined.
12. Presidential Decree 178/2014 - Government Gazette 281 / A / 31-12-2014, Organization of Greek Police Services, as amended by Presidential Decree 93/2020 - Government Gazette 219 / A / 13-11-2020
13. Law 4249/2014 Government Gazette A’ 73/24-3-2014
14. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013, replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013
15. Law 4411/2016 Government Gazette A’ 142 - 03.08.2016
16. Law 7001/2/1261-(21) dated 28.08.2009 common Ministerial decision of the Ministers of Interior, Economy and Finance and Justice (B’1879)
17. UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III)
18. UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999