Cybercrime law

Koops, E.J.; Robinson, T.

Published in:
Digital evidence and computer crime

Publication date:
2011

Document Version
Peer reviewed version

CYBERCRIME LAW – A EUROPEAN PERSPECTIVE

Bert-Jaap Koops and Tessa Robinson

This is a pre-print version of the Chapter published in: E. Casey (ed.), Digital Evidence and Computer Crime, 3rd ed., Waltham, MA etc.: Academic Press, p. 123-183.

Countries in Europe have fundamentally different legal systems, unlike the United States which at least share a common framework. Europe has countries with a common-law system (the United Kingdom and Ireland) as well as countries with a civil-law system (most Continental countries), which have different traditions in the sources of law.

Several initiatives are underway to increase consistency in legal frameworks between countries in Europe and to support law enforcement involving multiple jurisdictions. However, fundamental differences between common-law and civil-law criminal justice systems remain. Moreover, two supranational bodies – the European Union and the Council of Europe – influence cybercrime law in European countries, creating unique challenges for harmonisation and for dealing with this topic in a single chapter.

This chapter tackles the challenge in presenting a European perspective of cybercrime law by presenting the two major initiatives to increase consistency across countries, and by delving into two examples of the differing legal systems that exist in Europe. Specifically, this chapter sets down the European legal framework – in particular the Cybercrime Convention – and relevant national legislation and case examples from England, Ireland, and the Netherlands to illustrate key points. We start with a brief overview of the sources of European and national cybercrime law. We then focus on the various cybercrime offences – computer integrity crimes, computer-assisted crimes, content-related crimes, and some other offences. We end with a brief discussion of jurisdiction issues.

THE EUROPEAN AND NATIONAL LEGAL FRAMEWORKS

For the European legal framework on cybercrime, we have to look at two Europes, since both the the Council of Europe and the European Union are active in the field. The Council of Europe launched the most comprehensive initiative with the Convention on Cybercrime, but the European Union moves beyond that in some respects in an effort to better harmonise legislation in its member states (De Hert, González Fuster and Koops 2006).

The Council of Europe (CoE, see www.coe.int) is a pan-European international body with 47 member states, focusing on human rights, democracy, and the rule of law. For cybercrime, the Convention on Cybercrime (CETS 185, hereafter: 'Cybercrime Convention') stands out. Apart from CoE member states, other countries can accede to this convention as well. In addition to the Cybercrime Convention, some other instruments make up the European cybercrime legal framework, such as the Additional Protocol to the Cybercrime Convention on racism through computer systems (CETS 189) and the Lanzarote Convention on the protection of children against sexual abuse (CETS 201), as discussed later in this chapter.

The European Union (EU, see europa.eu) is a political union between 27 European countries, 16 of which currently make up the Euro zone. Its common objective is to offer a single market. The union is comparable to the Federal and State legal systems in the United States, although EU member states enjoy a greater degree of sovereignty. While EU legislation emanates from the European Parliament, the Council of Ministers, and the European Commission, it is incorporated by member state governments into domestic law. So, unlike federal laws in the United States,

which apply equally in all states, EU criminal legislation is implemented separately in each country, potentially leading to varying legislation.

The EU has recently undergone constitutional change with the Lisbon Treaty, which, inter alia, has increased the involvement of the European Parliament in efforts to harmonise criminal law. Nevertheless, criminal law is still to a large extent a matter of national rather than EU legislation, although the latter is gaining ground. For cybercrime, particularly relevant is the Framework Decision 2005/222/JHA on attacks against information systems (hereafter 'Framework Decision'), which criminalises certain computer-integrity crimes. This Framework Decision is discussed in the next section.

National Frameworks:Common-law and Civil-law

For the national law, we have chosen to discuss countries with different legal traditions: Ireland and England in the common-law tradition, and the Netherlands in the civil-law tradition. In common law countries, the law centres primarily on case-law, whereas in civil-law countries, statutory law plays a pivotal role; this is a matter of degree rather than an absolute difference, since in all countries, legislation and case-law are relevant for determining 'the law'. Another difference, again of degree, is that common-law countries like the UK and US have a more adversarial system in criminal law, focusing on the 'battle of arms' between prosecution and defense, with a relatively passive role for the judge, whereas civil-law countries like the Netherlands tend to have a more – although moderated in modern times – inquisitorial system in criminal law, with an active role for the judge to 'find the truth' in the case.

Ireland and England operate under common law systems. (Note that within the United Kingdom, Scotland operates a distinct legal system as does Northern Ireland. For the purpose of this analysis we have focused on the law of England and Wales, which for brevity's sake we will refer to as England.) Ireland has a written constitution. Both Ireland and the United Kingdom are members of the European Union and members of the Council of Europe. European Union law has supremacy over domestic law but is applied and interpreted by the domestic courts subject to appeal in some cases (i.e. on a point of European law where all domestic remedies have been exhausted) to the European Courts sitting in Luxembourg. Both jurisdictions have adopted the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") into domestic law and again in certain cases an appeal lies to the European Court of Human Rights in Strasbourg. In terms of influence, one jurisdiction on the other, English case law is deemed to be persuasive authority in Irish courts but never binding. Irish cases are sometimes cited before English courts as persuasive authority, though this is rarer.

Both jurisdictions operate an adversarial criminal justice system: the prosecution is required to prove all elements of an offence beyond a reasonable doubt. In the majority of cases, offences have a mental element – referred to as the *mens rea* (literally "guilty mind") – which contains the element of intent or recklessness as to consequences of the action, and the physical element – *actus reus* – which is the action (or omission) required in committing the offence. Offences are categorised as summary – or minor – offences which can be tried by the lower courts without a jury and attract lesser penalties, and indictable (i.e. tried on indictment) or non-minor offences, tried in the higher courts by a judge sitting with a jury and attracting higher penalties. In circumstances where an accused is to be tried summarily on a charge of an offence that is also indictable he or she may elect to have the case sent forward for trial by jury. Persons convicted and sentenced by a trial court may seek leave to appeal conviction and or sentence before the Court of (Criminal) Appeal. Rules of evidence and procedures have developed over the centuries

and are frequently tested before the courts of appeal, and the Strasbourg Court, the ECHR guaranteeing by Article 6(1) the right to a fair trial.

The Netherlands' system of criminal law also requires a mental element as well as a physical element – act or omission – to constitute an offence. It distinguishes between misdemeanours (Third Book of the Dutch Criminal Code ("DCC") and crimes (Second Book of the DCC). The Criminal Code has a system of maximum penalties, but does not use minimum penalties. Contrary to the common-law countries, the Netherlands does not have a jury system. The yardstick for conviction is that the trial judge has obtained the inner conviction that the defendant is guilty of the offence, based on the statutory means of evidence (article 338-339 Dutch Code of Criminal Procedure ("DCCP")).

Some cybercrimes have a rather low maximum penalty for simple cases and a higher maximum for aggravated instances, see for example hacking and data interference (*infra*). An often-used maximum is four years' imprisonment, since this is the general threshold to allow pre-trial detention (artticle 67(1) DCCP) and this in turn is a threshold for many investigation powers to be applied, like ordering delivery of (non-sensitive) personal data (article 126nd DCCP) or telecommunications traffic data (article 126n DCCP). However, because digital investigation powers may also be required for 'simple' cybercrimes, for example hacking without aggravating circumstances, the Computer Crime II Act inserted almost all cybercrimes specifically in article 67(1) DCCP. As a result, for any cybercrime, pre-trial detention is allowed regardless of their maximum penalty, and most investigation powers can be used to investigate the crime.

PROGRESSION OF CYBERCRIME LEGISLATION IN EUROPE

Criminal laws relating to computers and the Internet have developed differently over the years in various countries. To better understand the current laws and legal frameworks in Europe, it is useful to understand where they came from; their sources. English and Irish law build upon past case law as precedent, the written Constitution (in Ireland), European instruments, international covenants and domestic statutes. The main sources of Dutch law are domestic statutes and international treaties. The Dutch Constitution is not a direct source, since the courts are not allowed to determine the constitutionality of legislation (art. 120 Dutch Constitution); courts can, however, apply standards from international law, most visibly the ECHR, when deciding cases. For the interpretation of domestic statutes, the parliamentary history is a leading source, followed by case law (particularly from the Dutch Supreme Court) and by doctrinal literature.

To provide a general background for the specific issues dealt with later in this Chapter, we sketch here the overall progression of cybercrime legislation in England, Ireland and the Netherlands, as well as in the Council of Europe and the European Union.

Domestic Criminal Law Statutes

In 1990, England became the first European country to enact a law to address computer crime specifically. The Computer Misuse Act introduced three new offences: unauthorized access to a computer; unauthorized access with intent to commit or facilitate the commission of further offences; and unauthorized modification of computer material (ss. 1, 2, and 3). That statute has recently been amended by the Police and Justice Act 2006 (which came into force in October, 2008) and to some extent the Serious Crime Act 2007. The extent of the amendments will be discussed below. The UK Criminal Damage Act 1971 has also been applied to offences involving computer misuse. The content-related offences concerning child pornography are contained within the Protection of Children Act 1978 as amended by the Criminal Justice and Public Order

Act 1994. The statutes dealing with fraud and forgery are the Fraud Act 2006 and the Forgery and Counterfeiting Act 1981, and also relevant is the copyright legislation contained in the Copyright and Rights Related Acts.

Ireland has not yet enacted a specific computer crime statute. With the exception of the area of child pornography offences, very few if any computer crime prosecutions have been brought in that jurisdiction. Specific legislation as required by the EU Framework Decision on attacks against information systems has not yet been enacted although a Bill is reported to be in preparation and increasing awareness of the prevalence of computer-related crime will presumably result in more prosecutions being taken.

Offences involving computer integrity, offences assisted by computer misuse and content-related offences involving computer use are contained in the following Irish statutes: the Criminal Damage Act 1991, the Criminal Justice (Theft and Fraud Offences) Act 2001, the Electronic Commerce Act 2000, the Copyright and Related Rights Act 2000, the Child Trafficking and Pornography Act 1997 and the Criminal Justice Act 2006.

With respect to cybercrime legislation in the Netherlands, the most important laws are the Computer Crime Act (*Wet computercriminaliteit*) of 1993 (*Staatsblad* [Dutch Official Journal] 1993, 33) and the Computer Crime II Act (*Wet computercriminaliteit II*) of 2006 (*Staatsblad* 2006, 300). Both are not separate Acts, but laws that adapted the Dutch Criminal Code (DCC) (*Wetboek van Strafrecht*) and the Code of Criminal Procedure (DCCP) (*Wetboek van Strafvordering*). Besides these two major laws, several other laws adapting the Criminal Code and the Code of Criminal Procedure have been passed to regulate more specific forms of cybercrime. Both Codes are available in Dutch via www.wetten.overheid.nl. Case law is available in Dutch at www.rechtspraak.nl, indicated with reference numbers LJN. The most comprehensive up-to-date discussion of Dutch cybercrime legislation can be found in Koops (2007; 2010).

Council of Europe Convention on Cybercrime, and Protocol

In 2001, realizing that certain computer-related offences required special consideration, 26 member countries convened in Budapest and signed the Council of Europe Convention on Cybercrime to create “a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation” (recital 4 of the preamble to the Convention). Although the COE Convention on Cybercrime represents an aspirational policy document, a country that ratifies the Convention commits to putting in place a legislative framework that deals with cybercrime according to Convention requirements. Within this commitment, each country is given discretion in relation to the full scope, say, of a criminal offence, by defining its particular elements of dishonest intent or requiring that serious harm be done before an offence is deemed to have been committed.

The Convention on Cybercrime entered into force on the 1 July, 2004 and its status as of the 22 January, 2009 is that it has been signed by 46 States, and ratified by 23 including the United States of America (as a non-member state of the Council of Europe) where it entered into force on the 1 January, 2007, and the Netherlands, where it entered into force on the 1 March, 2007. It has been signed but not yet ratified by Ireland and the United Kingdom. Thus it does not have legal effect in those jurisdictions.

Concerned by the risk of misuse or abuse of computer systems to disseminate racist and xenophobic propaganda, the member states of the Council of Europe and other State Parties to the

Convention on Cybercrime agreed an additional protocol to the Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems on the 28 January, 2003. That protocol entered into force on the 1 March, 2006 and (as of September, 2009) has 34 signatories, 15 of whom have ratified it. Neither Ireland nor the United Kingdom have signed or ratified the protocol yet. Nonetheless, its provisions will be briefly examined in this part.

European Union Framework Decisions

EU Framework Decisions are an effort to bring some consistency in the area of justice and home affairs, including computer crime.

By Title VI of the Treaty on European Union (prior to the Lisbon Treaty), which contains the provisions on police and judicial cooperation in criminal matters, the Council of the European Union (made up of the justice ministers of the member states of the European Union), have the discretionary power under article 34(2)(b) of the Treaty, to "adopt framework decisions for the purpose of approximation of the laws and regulations of the member states. Framework decisions shall be binding upon the member states as to the result to be achieved but shall leave to the national authorities the choice of form and methods. They shall not entail direct effect."

The EU Council adopted Framework Decision 2005/222/JHA on attacks against information systems on the 24 February, 2005, with an objective "to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the member states, through approximating rules on criminal law in the member states in the area of attacks against information systems" (recital 1 of the preamble). It is recited in the preamble to the framework decision that "criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism" (recital 8) and that "significant gaps and differences in member states' law in this area may hamper the fight against organised crime and terrorism …The transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area." The Framework Decision entered into force on the 16 March, 2005.

In the area of computer-assisted crime and content-related crimes, the EU Council adopted Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment, which includes offences related to computers (article 3) and offences related to specifically adapted devices (article 4), which came into force on the 2 June, 2001, and adopted Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography which recognises that child pornography is increasing and spreading through the use of new technologies including the Internet (recital 5 of the Preamble) and has as its objective the harmonisation of offences and definitions throughout the EU, which came into force on the 20 January, 2004.

The Lisbon Treaty, if and when ratified, intends, by article 69B, that "the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis." The areas

of crime concerned are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

SPECIFIC CYBERCRIME OFFENCES

The remainder of this chapter provides an overview of cybercrime offences, following the structure of the Cybercrime Convention, illustrated with Irish, English, and Dutch statutory provisions or cases.

The Cybercrime Convention distinguishes between three categories of crime, which are roughly similar to those of the classic typology of Donn Parker (1973): computer-integrity crimes (where the computer is object of the offence), computer-assisted crimes (where the computer is an instrument), and content-related crimes (where the computer network constitutes the environment of the crime).

Computer-integrity crimes

The first category of offences concerns 'hard-core' cybercrime, criminalising offences against the confidentiality, integrity, or availability of computer data or computer systems.

The Council of Europe Convention on Cybercrime introduces the following five offences against the confidentiality, integrity and availability of computer data and systems.

1. illegal access, that is, intentional access to the whole or any part of a computer system without right (Article 2);
2. illegal interception, being the intentional interception without right made by technical means of non-public transmissions of computer data to, from or within a computer system (Article 3);
3. data interference, that is, the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right (Article 4);
4. system interference, being intentionally seriously hindering without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Article 5); and
5. misuse of devices, that is, the production, sale, procurement for use, import, distribution or otherwise making available of a device or password or access code with the intent that it be used for the purpose of committing any of the offenses established in articles 2–5 (Article 6).

"Computer system" is defined as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data", and "computer data" is defined as meaning "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".

The phrase "without right" is considered in the Explanatory Report to the Convention on Cybercrime issued by the Council of Europe (paragraph 38) as follows:

> A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without

> right" derives its meaning from the context in which it is used. Thus, without restricting how [contracting] parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the [contracting] party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised … It is left to the [contracting] parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

The EU Framework Decision on attacks against information systems (2005/222/JHA) uses an almost identical definition of "computer data" and defines "information system" in the same terms as "computer system" is defined in the Cybercrime Convention, with the addition of "computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance".

The Framework Decision requires member states to take necessary steps to ensure that the following are punishable as criminal offences, at least for cases which are not minor:

1. Illegal access to information systems, being intentional access without right (article 2);
2. Illegal system interference, being intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data without right (article 3);
3. Illegal data interference, being intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system without right (article 4)
4. Instigation, aiding and abetting and attempt in relation to 1, 2 and 3 above (article 5).

"Without right" is defined in the Framework Decision as meaning: "access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation".

The Framework Decision directs that such offences are punishable by effective, proportional and dissuasive criminal penalties (article 6(1)), and that offences referred to in articles 3 and 4 have a maximum penalty of at least between one and three years imprisonment, to be increased to a maximum of at least between two and five years imprisonment when committed with the framework of a criminal organisation (as defined).

Computer-assisted crimes
The second category of offences addressed by the Cybercrime Convention are computer-assisted crimes. Contrary to computer-integrity crimes, which are effectively new forms of crime that cannot be committed in the absence of computers or computer networks, and where the computer usually is the target of the crime, computer-assisted crimes are traditional crimes in which the computer is 'merely' a tool. They nevertheless merit attention from the legislator, if traditional crimes are formulated in a way that precludes their application to the digital world.

The EU Council Framework Decision on combating fraud and counterfeiting of non-cash means of payment directs member states to take necessary measures to ensure that two types of conduct – relating to computer use – are criminal offences when committed intentionally, being

- Offences related to computers (article 3): performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by:
  - without right introducing, altering, deleting or suppressing computer data, in particular identification data, or
  - without right interfering with the functioning of a computer programme or system.
- Offences related to specifically adapted devices (article 4): the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of:
  - instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsification of a payment instrument in order for it to be used fraudulently;
  - computer programmes for the purpose of which is the commission of any of the offences described as offences related to computer offences.

Content-related crimes
The third category of offences in the Cybercrime Convention relates to content-related crimes. They are similar to the computer-assisted crimes in that they relate to traditional offences and that computers are tools rather than targets, but they differ from them in that it is the content of data rather than the result of an action that is the core of the offence. The only content-related offence that the parties involved in drafting the Convention could agree upon, was child pornography. The other major candidate – racism – was not acceptable to the United States to include in the Convention, given the thrust of the First Amendment. As a consequence, racism was transferred to an Additional Protocol to the Convention, which parties can decide to sign at their own discretion.

COMPUTER INTEGRITY CRIMES

Hacking
The first and most obvious cybercrime is hacking or, in the Convention's term, 'illegal access': the intentional 'access to the whole or any part of a computer system without right' (art. 2 Convention; similarly, art. 2 Framework Decision). When implementing this provision, states may provide that hacking is only punishable when security measures are infringed, when committed with dishonest intent, or when the computer is part of a network.

Initially, the Dutch criminal provision (art. 138a DCC) criminalised hacking when a (minimal) security measure was infringed or the access was acquired through deceptive means. In 2006, however, the law was changed by changing these requirements from necessary conditions into sufficient conditions: i.e., infringing a security measure or acquiring access through deception are considered indications of unlawful access, but also normal access to an unprotected computers is considered hacking when done without right.

> CASE EXAMPLE: Press Services (LJN BG1503 and BG1507)
> An interesting illustration of 'without right' is the case of two ex-journalists who started working at the Dutch Ministry of Social Affairs (District Court The Hague, 24 October 2008, LJN BG1503 and BG1507). They used their old login names and passwords to

access the database of their former employer, Dutch Associated Press Services (GPD), and provided their minister with last-minute, unpublished, news from the database. When their login accounts expired, they used the login data from a former colleague still working at the GPD. The court considered accessing a database from a former employer a clear case of illegal access and convicted the ex-journalists to community service of 150 and 100 hours, respectively.

This case is actually a rare example of a conviction for hacking in the Netherlands; although the criminalisation of hacking dates from 1993, few hackers have been prosecuted or convicted to date.

The first offence under the UK Computer Misuse Act 1990, as amended, is your basic computer intrusion offence: hacking, which one commentator compares with breaking and entering (Gringas 2002, p. 285). Section 1(1) provides that:

A person is guilty of an offense if –

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
(b) the access he intends to secure is unauthorized; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.

The elements to be proved are that the perpetrator intended to break into the computer in the knowledge that he/she did not have authority so to do. The *actus reus* (the act or omissions that comprise the physical elements of a crime as required by law) is the action of breaking in (causing a computer to perform any function). Subsection (2) provides that

The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or date;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

The question of whether unauthorized use of a single computer came within the terms of the offence was examined by the English Court of Appeal in Attorney-General's Reference (No. 1 of 1991) [1992] 3 WLR 432 where, in answer to the point of law raised, namely "in order for a person to commit an offence under section 1(1) of the Computer Misuse Act 1990 does the computer which the person causes to perform any function with the required intent have to be a different computer from the one into which he intends to secure unauthorized access to any program or data held therein?" it was held that in section 1(1)(a) of the Act of 1990 the words "causes a computer to perform any function with intent to secure access to any program or data held in any computer," in their plain and ordinary meaning, were not confined to the use of one computer with intent to secure access into another computer; so that section 1(1) was contravened where a person caused a computer to perform a function with intent to secure unauthorized access to any program or data held in the same computer. Thus, for example, the (unauthorized) entering of a password into a computer system is sufficient to establish the offence.

The *mens rea* is the dishonest intent with knowledge of no authority.

The question of the meaning of the phrase *unauthorized access* in the Act has been tested in the English courts.

CASE EXAMPLE (D.P.P. v. BIGNELL 1998):
In this case, the court was concerned with a situation where police officers secured access to the police national computer for a non-police but rather personal use. The question was whether this amounted to commission of an offense contrary to section 1 of the 1990 Act. The court held that the defendants had authority to access the police computer even though they did not do so for an authorized purpose. Therefore, they did not commit an offense contrary to section 1 of the Act. The court noted in its judgment that the 1990 Act was enacted to criminalize the act of breaking into computer systems. Thus, once the access was authorized, the Act did not look at the purpose for which the computer was accessed.

The case gave rise to the question of whether the offence of unauthorized access might be extended to a situation of improper or illegal use by an authorized user. This question was considered by the House of Lords in R. v. Bow Street Magistrate (*ex parte* US Government, Allison) [1999] 3 W.L.R. 620 where they refined interpretation of the notion of authorized or unauthorized access.

CASE EXAMPLE (R. v. BOW STREET MAGISTRATE – ALLISON 1997):
Allison used credit card details obtained from American Express systems to commit US$1 million in ATM fraud. The defendant was accused of conspiring with legitimate employees of American Express to secure access to the American Express computer system with intent to commit theft and fraud, and to cause a modification of the contents of the American Express computer system. The Court of Appeal held that access was unauthorized under the Computer Misuse Act if (a) the access to the particular data in question was intentional; (b) the access in question was unauthorized by a person entitled to authorize access to that particular data; (c) knowing the access to that particular data was unauthorized. The court explained the decision as follows:

the evidence concerning [the American Express employee]'s authority to access the material data showed that she did not have authority to access the data she used for this purpose. At no time did she have any blanket authorization to access any account or file not specifically assigned to her to work on. Any access by her to an account which she was not authorized to be working on would be considered a breach of company policy and ethics and would be considered an unauthorized access by the company. The computer records showed that she accessed 189 accounts that did not fall within the scope of her duties. Her accessing of these accounts was unauthorized.… The proposed charges against Mr. Allison therefore involved his alleged conspiracy with [the employee] for her to secure unauthorized access to data on the American Express computer with the intent to commit the further offences of forging cards and stealing from that company. It is [the employee]'s alleged lack of authority which is an essential element in the offences charged.

The House of Lords noted that the court at first instance had felt constrained by the strict definition of unauthorized access in the Act and the interpretation put upon them by the court in D.P.P. v. Bignell. The House of Lords doubted the reasoning in Bignell but felt that the outcome was probably right. They went on to assert that the definition of unauthorized access in section 17 of the Act was open to interpretation, clarifying the offence as follows.

Section 17 is an interpretation section. Subsection (2) defines what is meant by access and securing access to any program or data. It lists four ways in which this may occur or be achieved. Its purpose is clearly to give a specific meaning to the phrase "to secure access". Subsection (5) is to be read with subsection (2). It deals with the relationship between the widened definition of securing access and the scope of the authority which

> the relevant person may hold. That is why the subsection refers to "access of any kind" and "access of the kind in question". Authority to view data may not extend to authority to copy or alter that data. The refinement of the concept of access requires a refinement of the concept of authorization. The authorization must be authority to secure access of the kind in question. As part of this refinement, the subsection lays down two cumulative requirements of lack of authority. The first is the requirement that the relevant person be not the person entitled to control the relevant kind of access. The word "control" in this context clearly means authorize and forbid. If the relevant person is so entitled, then it would be unrealistic to treat his access as being unauthorized. The second is that the relevant person does not have the consent to secure the relevant kind of access from a person entitled to control, i.e., authorize, that access.
>
> Subsection (5) therefore has a plain meaning subsidiary to the other provisions of the Act. It simply identifies the two ways in which authority may be acquired – by being oneself the person entitled to authorize and by being a person who has been authorized by a person entitled to authorize. It also makes clear that the authority must relate not simply to the data or program but also to the actual kind of access secured. Similarly, it is plain that it is not using the word "control" in a physical sense of the ability to operate or manipulate the computer and that it is not derogating from the requirement that for access to be authorized it must be authorized to the relevant data or relevant program or part of a program. It does not introduce any concept that authority to access one piece of data should be treated as authority to access other pieces of data "of the same kind" notwithstanding that the relevant person did not in fact have authority to access that piece of data. Section 1 refers to the intent to secure unauthorized access to any program or data. These plain words leave no room for any suggestion that the relevant person may say: "yes, I know that I was not authorized to access that data but I was authorized to access other data of the same kind." (pp. 626–627)

This situation is explicitly addressed by the US Computer Fraud and Abuse Act using the language "accessed a computer without authorization or exceeding authorized access".

Where the initial access is authorised but the subsequent purpose of the access or use of content is beyond what is authorised, it might be appropriate to prosecute under Data Protection legislation.

> CASE EXAMPLE: R. v Rooney [2006]
> Jacqueline Rooney obtained information from a police database relating to her sister's ex-boyfriend. The sister then used this information to bother her ex-boyfriend. The accused was convicted on counts of unlawful obtaining of personal data and unlawful disclosure of personal data contrary to section 55(1) of the Data Protection Act 1998 which conviction was upheld on appeal by the English Court of Appeal. The accused was employed in the human resources department of a police constabulary and as part of her duties she was authorised to access and view personal information about employees, for staff and work policing related purposes. The accused's sister had been in a relationship with a police officer which relationship broke down and the accused was found to have accessed the personal data of that police officer including his new address as well as data relating to his new girlfriend, also an employee of that police constabulary. She passed the information to her sister who used the information to make contact. The appeal related in part on the defence that she had accessed the information as part of her duties but the Court of Appeal found that she had abused her position and upheld the conviction.

The Police and Justice Act 2006 which effected amendments to the Computer Misuse Act has upgraded the hacking offence in section 1 by making it an indictable offence where originally it was a summary offence only. The maximum penalty on summary conviction now is 12 months imprisonment and/or maximum summary fine and the maximum penalty on conviction on indictment is two years imprisonment and or fine.

The second of the Computer Misuse Act offences concerning unauthorized access has the additional element of an intent to commit or facilitate the commission of further offences (section 2). It should be noted that a perpetrator may be guilty of this offence even where he/she has not in fact committed a further offence or indeed where the intended further offence would have been impossible to commit (section 2(4)). It is the intention that offends. Section 2(3) of the Act states that, "It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorized access or on any future occasion." The offence is triable summarily or on indictment, and on conviction on indictment the maximum penalty is five years imprisonment and or fine.

> CASE EXAMPLE: R. v Delamare [2003] 2 Cr. App. R. (S.) 80
> The case was heard by the English Court of Appeal as an appeal against the severity of sentence imposed. The accused had pleaded guilty to two counts of obtaining unauthorised access to computer material to facilitate the commission of an offence, contrary to s. 2(1)(b) of the Computer Misuse Act 1990. The facts were that the accused worked at a branch of Barclays Bank in England. He was approached by an old school acquaintance to whom he felt obligated, and asked to disclose details of bank account holders for £50 each. He disclosed details of two bank accounts. The matter came to light when a man impersonated one of the account holders and attempted to obtain $10,000 from the bank. Another man was waiting outside in a car and when that car was searched, documents relating to the bank account were found. The accused was interviewed and made a full confession. Concurrent sentences of eight months imprisonment were imposed by the trial court, whereas the two men caught at the bank were given non-custodial sentences. The Appeal court distinguished the offences noting that in the case of the accused there was, by way of aggravating factor, the breach of trust which he committed as a bank employee. Nonetheless, the Court reduced the sentence to one of four months detention in a young offender institution bearing in mind the accused's previous good character, plea of guilty and relative youth.

The basic hacking offence in Ireland is laid down in section 5 of the Criminal Damage Act 1991 which provides:

> (1) A person who without lawful excuse operates a computer—
>
> (a) within the State with intent to access any data kept either within or outside the State, or
>
> (b) outside the State with intent to access any data kept within the State,
>
> shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.
>
> (2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.

"Data" is defined by section 1 as meaning "information in a form in which it can be accessed by means of a computer and includes a program".

The *actus reus* of the offence is operating a computer without lawful excuse with intent to access data. It is not necessary to succeed in accessing data, and there is no requirement that any damage results from operating the computer without lawful excuse. The *mens rea* is the intent to access data, and the knowledge that the operating of the computer with that intent is without lawful excuse. The arguments that emerged in the English cases of *Bignell* and *Allison* in terms of whether the offence is committed if the operating of the computer is with lawful excuse but the data that is intended to be accessed is unauthorised to the user might arise, although *Allison* would be a persuasive authority against the argument in the Irish jurisdiction. Section 6 of the 1991 Act deals with the term "without lawful excuse", providing in subsection (2) as follows:

> A person charged with an offence to which this section applies [includes section 5 and section 2(1) discussed below] shall, whether or not he would be treated for the purposes of this Act as having a lawful excuse apart from this subsection, be treated for those purposes as having a lawful excuse—
>
> > (a) if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to consent to or authorise the damage to (or, in the case of an offence under section 5, the accessing of) the property in question had consented, or would have consented to or authorised it if he or they had known of the damage or the accessing and its circumstances,
> >
> > (b) in the case of an offence under section 5, if he is himself the person entitled to consent to or authorise accessing of the data concerned…

Illegal interception

Article 3 of the Convention criminalises the intentional 'interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system'. This includes intercepting electromagnetic radiation emanating from a computer screen or cables (TEMPEST).

In the Netherlands, illegal interception is criminalised in art. 139c DCC. This includes intercepting public telecommunications or data transfers in closed computer systems. It excludes, however, intercepting radio waves that can be picked up without special effort, as well as interception by persons with authorisations to the telecom connection, such as employers. Covert monitoring by employers of employees is only an offence if they abuse their power, but such cases have never been prosecuted; indeed, although employers often do not follow the guidelines for responsible monitoring by the Dutch Data Protection Authority, they usually get away with this in dismissal cases of employees who were found, for example, to be unduly interested in pornography during working hours (Cuijpers 2007). Besides art. 139c, several other provisions contain related penalizations; it is prohibited to place eavesdropping devices (art. 139d DCC), to pass on eavesdropping equipment or intercepted data (art. 139e DCC), and to advertise for interception devices (art. 441 DCC). Despite this comprehensive framework regarding illegal interception, very few cases are published in which illegal interception is indicted.

> CASE EXAMPLE: NTL [2003]
>
> NTL attempted to avoid complying with a police production order for stored emails by suggesting that to do so would involve committing the offence of illegal interception. The court disagreed, ruling that the authority to intercept was implicit in the production order.
>
> The case concerned interpretation of sections of the Regulation of Investigatory Powers Act 2000 in England. Section 1 of the 2000 Act provides so far as relevant:
>
> > "Unlawful interception

(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of …(b) a public telecommunication system.

(2) It shall be an offence for a person (a) intentionally and without lawful authority … to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system."

While conducting a fraud investigation, police sought and were granted a special production order from NTL, a telecommunications company, pursuant to the Police and Criminal Evidence Act 1984. NTL brought judicial review proceedings in relation to that order on the grounds that the material it held was held in confidence and to comply with the request would involve it committing an offence under section 1 of the 2000 Act. The facts were that NTL had a computer system which automatically stored emails from Internet service providers. Within its email client system, emails were routinely overwritten one hour after being read by the recipient. An unread email was kept for a limited period. Evidence was given that the only way that NTL could retain emails of customers on this system was to transfer a copy to a different email address from that of the intended recipient. The reviewing court held that it was implicit in the terms of the Police and Criminal Evidence Act that the body subject to an application by the police under that Act (i.e. NTL) had the necessary power to take the action which it had to take in order to conserve the communications by email within the system until such time as the court decided whether or not to make an order. That implicit power provided the lawful authority for the purposes of the 2000 Act and no offence would therefore be committed.

CASE EXAMPLE: R. v. E [2004] 1 WLR 3279

Police eavesdropping on one end of a telephone conversation does not amount to illegal interception and evidence obtained that way is admissible. In the course of an investigation into suspected drug dealing English police placed a covert listening device in the defendant's car which recorded words spoken by the defendant when in the car including his end of mobile telephone conversations. At a pre-trial hearing it was submitted on behalf of the defence that what had occurred was "interception" of the telephone calls contrary to section 2(2) of the Regulation of Investigatory Powers Act 2000, and that all evidence obtained through use of the listening device should be deemed inadmissible. The trial judge ruled against the submission but granted leave to appeal. The Court of Appeal dismissed the appeal holding that the natural meaning of the expression "interception" denoted some interference or abstraction of the signal, whether it was passing along wires or by wireless telegraphy, during the process of transmission. The recording of a person's voice, independently of the fact that at the time he is using a telephone, does not become interception simply because what he says goes not only into the recorder, but, by separate process, is transmitted by a telecommunications system.

The explanatory report of the Cybercrime Convention envisages that in some countries interception may be closely related to the offence of unauthorised access to a computer system. This would appear to be the position in Ireland at present; there is no specific offence expressly prohibiting illegal interception, and such would appear to come within section 5 of the Criminal Damage Act 1991 (see above). Covert Intelligence legislation, the Criminal Justice Surveillance Bill 2009, first stage, has been published (15 April, 2009), proposing inter alia to allow covertly intercepted communications to be used as evidence in criminal proceedings. It does not as

initiated (the process allows for amendments during the course of the debate stage) provide for specific regulation in relation to unlawful interception.

Data and system interference

Data interference is the intentional 'damaging, deletion, deterioration, alteration or suppression of computer data without right' (art. 4 Convention). Parties may pose a requirement of serious harm for this conduct to be punishable. A typical example are computer viruses that alter in any way certain data in a computer. Data interference is also covered by art. 4 of the EU Framework Decision, which uses similar language, with the addition of 'rendering inaccessible' computer data as an act of data interference.

System interference refers to the intentional 'serious hindering without right of the functioning of a computer system' through computer data (art. 5 Convention). This comprises computer sabotage, but also denial-of-service (DoS) attacks that block access to a system. It does not, however, criminalise spam – sending unsolicited, commercial or other, email –, except 'where the communication is intentionally and seriously hindered'; parties may, however, go further in sanctioning spam, for example by making it an administrative offence, according to the Explanatory Report (§69). System interference is also covered by art. 3 of the EU Framework Decision.

In Dutch law, data interference is penalised in art. 350a DCC. This includes deleting, damaging, and changing data, but it goes further than the European provisions by also including 'adding data' as an act of interference. Although adding data does not interfere with existing data as such, it does interfere with the integrity of documents or folders, so that it can be seen as a more abstract form of data interference. There is no threshold – even changing a single bit unlawfully is an offence – but minor cases will most likely not be prosecuted: Dutch criminal law applies the 'principle of opportunity', allowing the Public Prosecutor to decide, at their own discretion, when to prosecute.

If the interference was, however, committed through hacking and resulted in serious damage, the maximum penalty is higher, rising from two to four years' imprisonment (art. 350a(2) DCC). 'Serious damage' includes an information system not being available for several hours (Supreme Court, 19 January 1999, *Nederlandse Jurisprudentie* 1999, 25). Non-intentional (negligent) data interference is penalised by art. 350b DCC, if serious damage is caused, with a maximum penalty of one month's imprisonment.

Worms and computer viruses are considered a special case of data interference, being criminalised in art. 350a(3) DCC. The Computer Crime Act of 1993 used an awkward formulation to address viruses, which effectively only covered worms, but not viruses or Trojan horses; although it was generally assumed that the provision did cover all forms of malware through a teleological interpretation, the Computer Crime II Act of 2006 replaced it with a better formulation by describing viruses as data 'designated to cause damage in a computer'. Even though Trojans do not as such cause damage *per se* in a computer, they are covered by this provision, according to the parliamentary documents.

> CASE EXAMPLE: Kournikova
> A famous (or infamous) virus that originated from the Netherlands, was the Kournikova virus, inviting recipients to view an attached photograph of tennis starlet Anna Kournikova. The 19-year-old perpetrator, who was basically a script kiddie, was convicted by the Leeuwarden District Court (27 September 2001, LJN AD3861) of

intentional virus dissemination, and sentenced to 150 hours of community service. The verdict was upheld by the Supreme Court (28 September 2004, LJN AO7009).

System interference is penalised in various provisions in Dutch law, depending on the character of the system and of the interference. If the computer and networks are for the common good, intentional interference is punishable if the system is impeded or if the interference causes general danger to goods, services, or people (art. 161sexies DCC). Negligent system interference in similar cases is also criminalised (art. 161septies DCC). Even if no harm is caused, computer sabotage is still punishable when targeted at computers or telecom systems for the common good (art. 351 and 351bis DCC).

Whereas these provisions, all dating from the first wave of cybercrime legislation, concern computers with a 'public value', a relatively new provision concerns any computer interference. Art. 138b DCC was included in the Computer Crime II Act to combat 'e-bombs' and particularly DoS attacks: the 'intentional and unlawful hindering of the access to or use of a computer by offering or sending data to it'.

Although DoS attacks have thus been criminalised only in 2006, prosecutors and courts were able to apply the 'public-value' provisions to some DoS attacks before 2006. The blockers of several government websites used for official news – including www.regering.nl ('administration.nl') and www.overheid.nl ('government.nl') – were convicted on the basis of art. 161sexies DCC to conditional juvenile detention and community service of 80 hours (District Court The Hague, 14 March 2005, LJN AT0249). The District Court Breda, somewhat creatively, interpreted the hindering of an online banking service as constituting 'common danger to service provisioning' (30 January 2007, LJN AZ7266 and AZ7281). However, a DoS attack on a single commercial website was found not punishable under the pre-2006 law (Appeal Court 's-Hertogenbosch, 12 February 2007, LJN BA1891).

Spamming is not criminalised in the Criminal Code, but it is regulated in art. 11.7 Telecommunications Act with an opt-in system (or opt-out for existing customers); violation of this provision is an economic offence (art. 1(2) Economic Offences Act). The supervisory authority, OPTA, has fined spammers in several cases with considerable fines, including a fine of 10,000 EUR for an individual who had sent 12,400 sms spam messages in a single day (OPTA, 3 November 2008), and a fine of 75,000 EUR for an individual who had sent over 9 billion spam email messages (resulting in earnings of at least 40,000 EUR) (OPTA, 2 February 2007).

By section 3 of the English Computer Misuse Act 1990, as amended,

1. A person is guilty of an offence if—
   (a) he does any unauthorised act in relation to a computer;
   (b) at the time when he does the act he knows that it is unauthorised; and
   (c) either subsection (2) or subsection (3) applies.
2. This subsection applies if the person intends by doing the act—
   (a) to impair the operation of any computer;
   (b) to prevent or hinder access to any program or data held in any computer; or
   (c) to impair the operation of any such program or the reliability of any such data.
3. This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

This new version of the offence was inserted by the Police and Justice Act 2006 and came into force in October, 2008 (and only applies to offences where all of the elements were present/acts committed after that date – otherwise the old section 3 applies). This is the most serious of the offences under the 1990 Act and is punishable on conviction on indictment with a maximum sentence of ten years imprisonment. The amendment brings in the element of recklessness to the offence, thereby broadening the scope of the *mens rea* required to be proved. The *actus reus* is the doing of an unauthorised act in relation to a computer. The *mens rea* is intent as set out in subsection 2 or recklessness as to whether the action will do any of those things set out in subsection 2. Subsection 2 covers both system and data interference as an objective or intention of the unauthorised act. Again, applying the plain and ordinary meaning of the language used in the section, it is clear that the unauthorised act need not have succeeded in impairing or preventing or hindering as the case may be. The offence is in the act with the intent. No damage need arise for the offence to have been committed. Indeed, subsection (4) specifies that the intention or recklessness need not even be directed at any particular computer, program or data, or a program or data of any particular kind.

The previous wording of the Act was narrower in scope, making it an offence to do any act which causes an unauthorised modification of the contents of any computer, having the requisite intent and the requisite knowledge at the time of the doing of the act.

> CASE EXAMPLE Zezev and Yarimaka [2002]
> The first accused was employed by a company in Kazakhstan which was provided with database services by Bloomberg L.P., a company which provided news and financial information through computer systems worldwide. The accused gained unauthorised access to functions of Bloomberg's computer system. In doing so they were able to access the email accounts of the company's founder and head of security. They sent emails indicating that the company's system had been compromised and demanded payment of $200,000 or they would publicise the system's breach. The company founder contacted the FBI and it was arranged that he would meet the accused in London. Discussions took place and were covertly recorded. The accused were arrested, and the United States sought their extradition, inter alia on a charge that they had conspired with each other to cause an unauthorised modification of computer material in Bloomberg's computer system. There was evidence that the accused would use the computer so as to record the arrival of information which did not come from the purported source. The accused contested the extradition contending that the wording of section 3(2)(c) of the 1990 Act (as it then was prior to amendment by the Act of 2006) "to impair the operation of any such program or the reliability of any such data" confined the offence under section 3 to those who damaged the computer so that it did not record the information which was fed into it. The feeding into a computer of information that was untrue did not "impair the operation" of the computer. The court rejected this argument, holding that it was clear that if a computer was caused to record information – undoubtedly data – which showed that it came from one person, when it in fact came from someone else, that manifestly affected its reliability.

> CASE EXAMPLE Lennon [2006]
> An email bombardment may amount to unauthorised modification – even though there is no corruption of data – where the emails are sent for the purpose of interrupting the proper operation and use of the system. This English case was a prosecution under section 3(1) of the 1990 Act prior to its amendment which prohibited the unauthorised modification of the contents of a computer. The accused sent emails to a former employer using a "mail-bombing" program called Avalanche V3.6 which he downloaded from the

internet. The mail was set to "mail until stopped". The majority of the emails purported to come from the company's human resources manager. It was estimated that the accused's use of the program caused some five million emails to be received by the company's email servers. The trial judge ruled that there was no case to answer and dismissed the charge on the basis that section 3 was intended to deal with the sending of malicious material such as viruses, worms and Trojan horses which corrupt or change data, but not the sending of emails and that as the company's servers were configured to receive emails, each modification occurring on the receipt of an email sent by the accused was authorised. The prosecution appealed the trial judge's ruling and it was held by the Court of Appeal that the owner of a computer which is able to receive emails is ordinarily to be taken as consenting to the sending of emails to the computer. But that implied consent given by a computer owner is not without limit: it plainly does not cover emails which are not sent for the purpose of communication with the owner, but are sent for the purpose of interrupting the proper operation and use of his system. There was a case to answer and the case was remitted to the trial court for hearing.

CASE EXAMPLE Vallor [2004]
In a more clear cut case, Vallor was found guilty of violating the Computer Misuse Act 1990 after he created and spread malicious programs on the Internet. This case came before the English Court of Appeal as an appeal of severity of sentence. The accused pleaded guilty to three offences of releasing computer viruses onto the internet under section 3 of the 1990 Act. On three occasions over a period of about six weeks, the accused wrote a virus code and sent it out on the internet where it travelled through emails. The first virus was detected in 42 different countries and had stopped computer systems 27,000 times. The second and third viruses operated as a worm arriving in an email message, and were programmed to bring the operation of computers to a stop; when they were rebooted, they removed all material which had not already been saved. A user name was traced through postings to various internet bulletin boards and that user name was traced by the computer crime unit to an internet access account register to the accused at his home address. The accused was sentenced to concurrent sentences of two years imprisonment. On appeal the court upheld the sentence finding that the sentencing court was correct in indicating that the offences involved the actual and potential disruption of computer use on a grand scale: the offences were planned and deliberate, calculated and intended to cause disruption, and the action was not isolated but a persistent course of conduct.

In Ireland, these offences would be prosecuted under the Criminal Damage Act 1991 which provides in section 2(1) that:

> A person who without lawful excuse damages any property belonging to another intending to damage any such property or being reckless as to whether any such property would be damaged shall be guilty of an offence.

The offence is indictable and carries a maximum penalty on conviction on indictment of a term of imprisonment of ten years. Both data and system interference are covered by the wording, and the reckless element is included in the mens rea element. "Property" is defined in the Act (section 1(1)) as meaning (a) property of a tangible nature, whether real or personal … and (b) data.

CASE EXAMPLE (R. v. WHITELEY 1991):
This English case occurred prior to the Computer Misuse Act and was prosecuted under the Criminal Damage Act, 1971. The defendant had broken into the Joint Academic

> Network system, a network of connected ICL mainframe computers at universities, polytechnics and science and engineering research institutions. The defendant deleted and added files, put on messages, made sets of his own users and operated them for his own purposes, changed the passwords of authorized users and deleted files that would have recorded his activity. He successfully attained the status of systems manager of particular computers, enabling him to act at will without identification or authority.
>
> Under the Criminal Damage Act, the defendant was charged with causing criminal damage to the computers by bringing about temporary impairment of usefulness of them by causing them to be shut down for periods of time or preventing them from operating properly and, distinctly, with causing criminal damage to the disks by way of alteration to the state of the magnetic particles on them so as to delete and add files – the disks and the magnetic particles on them containing the information being one entity and capable of being damaged. The jury acquitted the defendant of the first charge and convicted on the second. The defense appealed the conviction to the Court of Appeal on the basis that a distinction had to be made between the disk itself and the intangible information held upon it which, it was contended, was not capable of damage as defined in law (at that time).
>
> The Court of Appeal held that what the Criminal Damage Act required to be proved was that tangible property had been damaged, not necessarily that the damage itself should be tangible. There could be no doubt that the magnetic particles on the metal disks were a part of the disks and if the defendant was proved to have intentionally and without lawful excuse altered the particles in such a way as to impair the value or usefulness of the disk, it would be damage within the meaning of the Act. The fact that the damage could only be detected by operating the computer did not make the damage any less within the ambit of the Act.

A word on recklessness: Smith and Hogan, Criminal Law (12th ed, OUP, 2008) at pp. 107 to 108, discussing recklessness as a form of *mens rea*, state:

> For many crimes, either intention to cause the proscribed result or recklessness as to whether that result is caused is sufficient to impose liability. A person who does not intend to cause a harmful result may take an unjustifiable risk of causing it. If he does so, he may be held to be reckless. …
> The standard test of recklessness … requires not only proof of a taking of an unjustified risk, but proof that the defendant was aware of the existence of the unreasonable risk. It is a subjective form of mens rea, focused on the defendant's own perceptions of the existence of a risk.
> [Cunningham [1957] 2 QB 396]

Following DPP v Murray [1977] IR 360, the definition contained in s. 2.02(2)(c) of the American Model Penal Code constitutes the definition of recklessness in Irish Law:

> "A person acts recklessly with respect to a material element of an offence when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that, considering the nature and purpose of the actor's conduct and the circumstances known to him, its disregard involves culpability of high degree".

In Ireland, acts of advertent risk taking amount to recklessness (subjective test). This was recently confirmed by the Irish Supreme Court in DPP v Cagney and McGrath [2007] IESC 46.

Misuse of devices

Article 6 of the Convention criminalises 'misuse of devices', which includes hardware as well as software and passwords or access codes. It is aimed at combating the subculture and black market of trade in devices that can be used to commit cybercrimes, such as virus-making or hacking tools. 'To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences' (Explanatory Report, § 71). Article 6 is a complex provision, establishing

> as criminal offences under its domestic law, when committed intentionally and without right:
> a) the production, sale, procurement for use, import, distribution or otherwise making available of:
>> (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
>> (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
>
> with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
> b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5.

The key clauses here are that devices *primarily* made to commit cybercrimes, and any *access code* usable to commit a cybercrime, cannot be *procured* or *possessed* if one has the *intent to commit a cybercrime*. According to the Explanatory Report (at §73), 'primarily designed' will usually, but not absolutely, exclude dual-use devices (i.e., having both a lawful and an unlawful purpose); the device's 'primary design' purpose is to be interpreted objectively, not subjectively. Unfortunately, the Report does not indicate how 'intent to commit a crime' is to be proven; the clause was added to prevent overbroad criminalisation (§76), in order to avoid, for example, forensic or information-security professionals who also need such tools to operate under the threat of criminal law. It might however be difficult to prove in practice that a possessor of a virus tool or someone else's password has intent to commit a cybercrime. Courts should not assume such intent on the basis of the fact of possession itself; other evidence must be found that the person indeed is planning to commit a cybercrime.

In Dutch law, misuse of devices has been penalised through the Computer Crime II Act in art. 139d(2-3) DCC: this covers misuse of devices or access codes with intent to commit hacking, e-bombing or DoS attacks, or illegal interception. Misuse of devices or access codes with intent to commit computer sabotage (as in art. 161sexies(1)) is covered by art. 161sexies(2) DCC. An omission of the legislator seems to be the misuse of devices with intent to spread a computer virus; this is covered by the Cybercrime Convention, but the target offence of virus-spreading in art. 350a(3) DCC is not included in the new provisions on misuse of devices.

In England, the Police and Justice Act 2006 created a new set of offences concerning the misuse of devices, inserting section 3A into the 1990 Act in the following terms:

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
(4) In this section "article" includes any program or data held in electronic form.

The offences under section 3A can be tried summarily on or indictment, and the maximum sentence on conviction on indictment is a term not exceeding two years imprisonment.

The question still arises as to whether mere possession of malicious code, or devices such as keyloggers, etc, is an offence.

The following two cases were prosecuted under the original section 3 of the 1990 Act (as inchoate offences, i.e. attempt, aiding and abetting or inciting commission of an offence) but could now, once all of the acts and elements were committed after October, 2008, be prosecuted under the new section 3A. They might also be considered examples of illegal interception as that offence is envisaged by the Cybercrime Convention (noted above).

CASE EXAMPLE Maxwell-King [2001]
The accused and his company manufactured and supplied what are known as general instrument devices which, when fitted to a general instrument set-top box, would allow the upgrading of the analog cable television service provided so that the subscriber to the cable television service would be permitted to access all channels provided by the cable company regardless of the number of channels or number of programmes for which the subscriber had paid. At the time the offences were committed there was no device available to the companies, as the court stated, to "indulge in what is know as 'chip-killing' by which the companies can send a signal down the cable which effectively disables and kills the chip which has been inserted by means of the device provided". The accused pleaded guilty to three counts of inciting the commission of an offence contrary to section 3 of the 1990 Act, and was sentenced to four months imprisonment. The accused appealed the severity of the sentence. It was held by the Court of Appeal that the offence was effectively a form of theft and plainly an offence of dishonesty. However a conviction on a plea of guilty for a first offence of this nature committed on a small scale (only 20 devices had been supplied over a period of three months with an estimated turnover of £600) did not necessarily cross the threshold of seriousness which required the imposition of a custodial sentence. The sentence was varied to 150 hours of community service.

CASE EXAMPLE Paar-Moore [2003]
This was another example of the accused making and distributing devices known as cable cubes, which allowed persons who subscribed to cable television services to view channels for which they had not paid the subscription. According to the judgment of Sir Richard Rougier, at paragraph 3,

> The appellants, somewhat disingenuously, used a written disclaimer, which apparently had been taken from an American internet site, the purpose of which was an attempt to absolve them from liability, saying that if the customer was not

> sure about whether or not the device was legal he should not use it. In our judgment, so far from absolving the appellants from criminal liability, it serves to illustrate their realisation that their trade was almost certainly illegal.
>
> The sentencing court sentenced the accused to seven months imprisonment and the accused appealed the severity of that sentence to the Court of Appeal, arguing, relying on Maxwell-King [2001], that the offence did not pass the custody threshold, and or that even if it did, seven months imprisonment was excessive. The court held (paragraph 8) that
>
> > This type of offence is a serious matter, compromising, as it does, the integrity of the cable network system in this country, and because of that and because of the obvious danger of rapid expansion of the popularity of this type of offence it was one that needed stamping on at the outset.
>
> However, the court went on to agree with the accuseds' second argument that the period of imprisonment was excessive and that a shorter period for persons who were effectively of good character, and representing no more that the 'clang of the prison gates', would be a sufficient deterrent and would satisfy the public demand for justice. A period of four months imprisonment was imposed.

In Ireland, the misuse of devices as a computer integrity crime (as envisaged by the Cybercrime Convention) is not expressly set down in legislation in those terms. An offence of this type would probably be caught by section 4(a) of the Criminal Damage Act 1991 which prohibits the possession of any thing with intent to damage property:

> A person… who has any thing in his custody or under his control intending without lawful excuse to use it or cause or permit another to use it—
>
> > (a) to damage any property belonging to some other person …
>
> shall be guilty of an offence.

The maximum penalty on conviction on indictment is a term of imprisonment not exceeding ten years. The *actus reus* is possession of the "thing". The *mens rea* involves intent, without lawful excuse, to use the thing or cause or permit another to use it to damage the property of another.

In the specific area of electronic signatures and signature creation devices, the Irish Electronic Commerce Act 2000 prohibits by section 25 misuse of that type of device. "Signature creation device" is defined as meaning a device, such as configured software or hardware used to generate signature creation data. The offence can be tried summarily or on indictment and the maximum sentence on conviction on indictment is imprisonment for a term not exceeding 5 years.

COMPUTER ASSISTED CRIMES

Forgery

Art. 7 of the Cybercrime Convention criminalises computer-related forgery: the intentional and unlawful 'input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.' Parties may pose a requirement of dishonest intent.

In Dutch law, computer-related forgery falls within the scope of the traditional provision on forgery ("*valsheid in geschrifte*", literally: forgery in writing), art. 225 DCC, which carries a maximum penalty is six years' imprisonment.

CASE EXAMPLE: Rotterdam computer fraud
In a landmark case, the term 'writing' (*geschrift*) in this provision was interpreted as covering computer files. This 'Rotterdam computer fraud' case (Dutch Supreme Court, 15 January 1991, *Nederlandse Jurisprudentie* 1991, 668) concerned an administrative civil servant working for the municipality of Rotterdam, who added fraudulent payment orders to the automated payment accounts system. The court formulated two criteria for a computer file to serve as a 'writing' in the sense of art. 225 DCC: it should be fit to be made readable (i.e. the electronic or magnetic signs should be translatable into any understandable language, include computer languages), and it should be stored on a medium with sufficient durability. Even though in the present case, the fraudulent orders were inserted in a temporary, intermediate file that only existed for a few minutes, the court held that the file had a legal purpose, since it was an essential link in the chain of proof of the accounts system, and that under these circumstances, the file was stored with sufficient durability.

Apart from the general provision on forgery, there is a specific penalisation of forgery of payment or value cards (art. 232 DCC). In the Computer Crime II Act, this provision was extended to cover all kinds of chip cards that are available to the general public and that are designed for payments or for other automated service provisioning. This provision has been used in several cases to prosecute phone debit-card fraud and skimming.

The forgery offence in Ireland and England/Wales is set out in similar terms respectively in the Criminal Justice (Theft and Fraud Offences) Act 2001, ss. 24 and 25, and the Forgery and Counterfeiting Act 1981, ss. 1 and 8.

By s. 25(1) of the 2001 Act,

> A person is guilty of forgery if he or she makes a false instrument with the intention that it shall be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person.

"Instrument" is defined as any document whether of a formal or informal character which includes any,

> Disk, tape, sound track or other device on or in which information is recorded by mechanical, electronic or other means.

Computer-related forgery offences would also come in under s. 9 of the 2001 Act (discussed above) which contains the general prohibition of wrongful use of a computer, and in the English jurisdiction, under s. 2 of the Computer Misuse Act 1990 which prohibits unauthorised access with intent to commit further offences.

Notably the offence of forgery contains a double intent in that the *mens rea* required for the commission of the offence to be proved involves both

(a) the intention that the false instrument be used to induce another to accept it as genuine, and
(b) the intention that by reason of so accepting it that other person does some act or makes some admission to their or another's prejudice.

CASE EXAMPLE: R v Gold and Schifreen [1988] AC 1063

This is an English 'computer hacking'-type case that was taken before enactment of the Misuse of Computers Act 1990. As can be seen from the facts below, the circumstances would now readily be caught as offences under the 1990 Act.
The accused were convicted of a number of offences under the Forgery and Counterfeiting Act 1981. They successfully appealed their convictions to the Court of Appeal, and the prosecution then sought and was granted leave to appeal that decision in the House of Lords on points of law of general public importance.
The indictment on which the accused were convicted contained specimen counts in similar terms alleging that they:

> "made a false instrument namely a device on or in which information is recorded or stored by electronic means with the intention of using it to induce the Prestal Computer to accept it as genuine and by reason of so accepting it to do an act to the prejudice of British Telecommunications plc."

The accused had gained unauthorised access to the Prestal computer by using the customer identification numbers and passwords of others without their permission. Having gained such access they obtained information to which they were not entitled, made unauthorised alterations to stored data and caused charges to be made to account holders without their knowledge or consent.
One of the points of law raised for consideration by the House of Lords was

> "Whether on a true construction of sections 1, 8, 9 and 10 of the Forgery and Counterfeiting Act 1981, a false instrument is made in the following circumstances - (a) a person keys into part of a computer (the user segment) a customer identification number and password of another, without the authority of that other, (b) with the intention of causing the same computer to allow unauthorised access to its database, and (c) the user segment, upon receiving such information (in the form of electronic impulses), stores or records it for a very brief period whilst it checks it against similar information held in the user file of the database of the same computer."

The House of Lords held that the process did not amount to the recording or storage of the customer identification number and password within the meaning of the 1981 Act in that the 'recording or storage' was not of a lasting and continuous nature, and that the *actus reus* of making a false instrument was not made out. The prosecution's appeal was dismissed.

Fraud

Like forgery, fraud can also be committed with the assistance of computers: the intentional and unlawful 'causing of a loss of property to another person by [interfering with computer data or a computer system] with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person' (art. 8 Convention). The term 'loss of property' is used here as a broad notion, comprising loss of money, tangibles, and intangibles with an economic value (§88 Explanatory Report).

In the Netherlands, computer-related fraud falls within the scope of the traditional provision on fraud or obtaining property through false pretences (*oplichting*), art. 326 DCC, with a maximum penalty of three years' imprisonment. For example, the unauthorized withdrawing of money from an ATM with a bank card and pin-code is fraud (Dutch Supreme Court, 19 November 1991, *Nederlandse Jurisprudentie* 1992, 124). The Computer Crime Act of 1993 added that fraud includes the falsely obtaining of computer data that have economic value in the regular market (*geldswaarde in het handelsverkeer*), such as computer programs or address databases. However, the falsely obtaining of pin codes or credit card numbers was not covered by the provision, as these data are not tradable on the regular market but only on black markets. As a result, phishing for financial data did not constitute fraud if financial data were merely being collected without being used. This lacuna in criminalisation was only amended in September 2009, when an

omnibus anti-terrorism Act (*Staatsblad* 2009, 245) replaced the phrase 'data that have economic value in the regular market' was replaced by simply 'data'.

Other fraud-related offences that also cover computer-related crime are extortion (art. 317 DCC) and blackmail (art. 318 DCC). The provision on extortion used a similar clause as fraud, but here, the clause 'data that have economic value in the regular market' was already replaced by 'data' in 2004 (*Staatsblad* 2004, 180), so that it includes the obtaining of pin codes and other data under threat of violence. For blackmail, this clause was changed by the aforementioned anti-terrorism Act in 2009.

A special case of fraud is telecommunications fraud, which is specifically penalised in art. 326c DCC: the use of a public telecommunications service through technical means or false signals, with the intention of not fully paying for it, which is punishable with up to three years' imprisonment.

Although theft – taking away property – will not usually be covered by art. 8 Convention, if property is lost through manipulation of a computer, it falls within the scope of computer-assisted fraud. An interesting issue in Dutch law is the question whether computer data can be considered 'property' (*goed*). After extensive academic debates, a controversial court case (Appeal Court Arnhem, 27 October 1983, *Nederlandse Jurisprudentie* 1984, 80), and recommendations by an legislative advisory committee, with the Computer Crime Act of 1993, the legislator decided against interpreting 'property' as comprising computer data, because computer data are not unique but 'multiple' and the product of mental rather than physical labour. Hence there was a need to adapt legislation by, for example, the specific insertion of 'data with an economic value' besides 'goods' in the fraud-related articles mentioned above.

> CASE EXAMPLE: computer data are not 'goods'
> The dogmatic issue whether computer data can or cannot be regarded as 'goods' did not reach the Dutch Supreme Court until 1996. In a landmark case, the court decided that computer data could not be the object of embezzlement (Dutch Supreme Court, 3 December 1996, *Nederlandse Jurisprudentie* 1997, 574). A system administrator had taken home computer disks with a complete back-up of the data from his employer's computer system. He was indicted with embezzlement, the unlawful appropriation of a good that is the partial or entire property of someone else and that he possesses other than through a crime (Article 334 and 335 of the Aruban Criminal Code – Aruba is part of the Kingdom of the Netherlands, with separate legislation that falls under the jurisdiction of the Dutch Supreme Court). The Supreme Court found that computer data cannot be embezzled, since they are not a 'good': "After all, a 'good' as mentioned in these provisions has the essential property that the person who has actual control over it, necessarily loses this control if some else takes over actual control. Computer data lack this property." Hence, data cannot be stolen or embezzled. This did not help the defendant, however, since the court subsequently interpreted the facts as embezzlement of *carriers* of computer data, and the Court of Appeal's conviction of the defendant was upheld.

However, with the advent of virtual worlds like Second Life and World of Warcraft, in which data constituting virtual property increasingly seems to acquire economic value, the courts may have to revise this doctrine.

> CASE EXAMPLE: Theft in Runescape

> A first Dutch case has been published that uses a new interpretation of 'goods'. Two boys playing the multiplayer online role-playing game of Runescape joined another boy to his home, where they hit the boy and forced him to log on to the game. They subsequently pushed him away from the computer and transferred a virtual amulet and mask from the victim's account to their own account. The District Court Leeuwarden (21 October 2008, LJN BG0939) held that the two boys had stolen goods, since the data were unique (only one person could possess them at one point in time) and had economic value.

This case has been endorsed in the literature as a sensible re-interpretation of the doctrine on 'computer data as goods' (Hoekman and Dirkzwager 2009). It will be interesting to see whether, and if so in what kinds of circumstances, other courts will follow this line.

The Fraud Act of 2006 updated the law in England. Section 2 sets out the offence of fraud by false representation:

> 2.—(1) A person is in breach of this section [and thereby is guilty of fraud according to section 1] if he
>
> (a) dishonestly makes a false representation, and
>
> (b) intends, by making the representation—
>
> (i) to make a gain for himself or another, or
>
> (ii) to cause loss to another or to expose another to a risk of loss.
>
> (2) A representation is false if—
>
> (a) it is untrue or misleading, and
>
> (b) the person making it knows that it is, or might be, untrue or misleading.
>
> (3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—
>
> (a) the person making the representation, or
>
> (b) any other person.
>
> (4) A representation may be express or implied.
>
> (5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Significant in this context is subsection (5) which covers deception of a system or device and allows for situations where there is not human intervention in receiving, conveying or responding to communications.

The offence may be tried summarily or on indictment and the maximum penalty on conviction on indictment is a term of imprisonment not exceeding 10 years. Fraud is a specified serious offence within schedule 1 of the Serious Crime Act 2007 which enables the court (on conviction on indictment) to make a serious crime prevention order. The serious crime prevention order is a new feature in English law. It is a form of civil injunction – like a high-end anti-social behaviour order – which imposes restrictions (including where an individual can live and can limit work and travel arrangements) on individuals and organizations convicted of being involved in serious crime, that may be made by the court where it has reasonable grounds to believe that the order would protect the public by preventing, restricting or disrupting involvement by the person in serious crime.

The offence of fraud by false representation is committed when the representation is made; it is not dependent on a result being achieved. According to Archbold, 2009,

> The representation can be made to a machine (section 2(5)), but is only so made when "submitted"; by analogy, it is submitted that a representation made by email will not be made until the email is sent. (Paragraph 21.372.)

The person making the representation must be shown to know, at the time of the making of the representation, that it is or might be untrue or misleading.

In respect of "phishing", Archbold, 2009 observes the following at paragraph 21.381:

> The explanatory notes to the Act state that the offence of fraud by false representation would be committed by someone who engaged in "phishing" by disseminating an email to a large group of people falsely representing that it had been sent by a legitimate financial institution and prompting the reader to provide information such as credit card and bank account numbers so that the "phisher" could gain access to others' assets (*sed quaere* whether the "phisher" would intend, by that representation, to make a gain in money or other property, or whether that intention would instead accompany a subsequent representation made to the financial institution using the information provided).

In addition to prohibiting the traditional offences of theft (the dishonest appropriation of property without the consent of its owner and with the intention of depriving its owner of it) and making or gaining loss by deception, the Irish Criminal Justice (Theft and Fraud Offences) Act, 2001, in section 9, tackles computer-related fraud and forgery by creating the offence of unlawful use of a computer in the following terms:

> A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

The actus reus is the dishonest operation of or causing to be operated a computer within the State. While the act can be committed within or outside the State, for the offence to be committed the computer to be operated must be located within the State. The mens rea is in the dishonesty and with the intention to make a gain or cause a loss. "Dishonestly" is defined in section 2 as meaning "without a claim of right made in good faith": in other words, the operation or causing to be operated of the computer is unauthorised and known to be so by the operator. The added element, making it a theft or fraud offence as distinct from unauthorised use of a computer, is the intention to make a gain or cause a loss.

CONTENT-RELATED CYBERCRIMES

Child pornography

Offences relating to the possession and distribution of child pornography are probably the most litigated and certainly the most notorious of cyber offences. Art. 9 of the Convention stipulates that the production, making available, distribution, procurement, and possession of child pornography should be criminalised when committed through use of computers. Parties can, however, decide not to criminalise procurement or possession. The age limit for child pornography advised by the Convention is 18 years; it must in any case be at least 16 years (art. 9(3)). An important innovation is that also 'virtual child pornography' is criminalised: computer-generated or computer-morphed images made to look like child pornography, in the Convention's terminology: 'realistic images representing a minor engaged in sexually explicit conduct' (art. 9(2)). The rationale of this is not so much direct protection against child abuse, since no children need to be actually abused for virtual images, but to prevent that such images 'might be used to

encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse' (§102 Explanatory Report). In January, 2004 the EU Council adopted Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography: outline offences.

In Dutch law, child pornography is penalised in art. 240b DCC, carrying a maximum penalty of four years' imprisonment. This includes the manufacture, distribution, publicly offering, and possession of pictures that show a minor in a sexual act. In 2002, the age limit was raised from 16 to 18 years, and to implement the Cybercrime Convention virtual child pornography was included in art. 240b as sexual images 'seemingly involving a minor' (*Staatsblad* 2002, 388).
To date, only one case has been published of criminal virtual child pornography.

> CASE EXAMPLE: Cartoon movie as virtual child pornography
> A man possessed a cartoon movie, 'Sex Lessons for Young Girls', showing a young girl engaged in sexual activity with an adult man. The District Court 's-Hertogenbosch (4 February 2008, LJN BC3225) considered this 'realistic' because an average child would not be able to distinguish between real and cartoon people. The 'average child', in this court's opinion, is a relevant yardstick for cartoon movies like this one that are intended – as indicated by the title and form – as a sex course for young children. A conviction for virtual child pornography therefore fitted the rationale of combating a subculture that promotes child abuse. The particular circumstances of the case – such as the title of the movie and the fact that it was actually shown to a young child – are likely to have played a role in the stress put in this decision on the rationale of combating a subculture of child abuse.

To date, this is the only conviction for virtual child pornography in the Netherlands, and it remains to be seen whether in future cases courts will adopt this court's using the perspective of a minor to interpret the term 'realistic'.

In January 2010, another computer-related activity in relation to child pornography was criminalised in the Netherlands, by an Act (*Staatsblad* 2009, 544) that implemented the Lanzarote Convention (CETS 201). Art. 240b DCC was extended with a criminalisation of intentional obtaining access to child pornography by means of a computer or communications service. The main reason for the expansion is that the Internet increasingly allows the 'consumers' of child pornography to watch it online without storing the pictures, thereby effectively circumventing the act of criminal possession of child pornography. A crucial threshold for criminal liability in this respect is 'intentional' (or, in the Convention's terms, 'knowingly'): to prevent users from being held liable if they only accidentally come across child pornography while surfing the net, the prosecution will have to prove that the obtaining access was done purposefully. The Explanatory Memorandum suggests that intentionality can be proven, for example, by the user paying for access, by the name of a hyperlink clicked on by the user, or by the user revisiting a website on which he has seen child pornography on a first visit. Since the legislator adopted the term 'intentionally' (*opzettelijk*) rather than 'deliberately' (*welbewust*) – which had been advised by the Public Prosecutor – the lower threshold of intention applies, i.e. 'conditional intention' (*voorwaardelijk opzet*): someone is criminally liable if he knows that an act on the Internet can lead to his accessing child pornography and he nonetheless takes a substantial risk that this will occur.

The law in England on child pornography predates the Cybercrime Convention and did not specifically mention computers. Section 1 (1) of the Protection of Children Act, 1978 as amended by the Criminal Justice and Public Order Act, 1994 makes it an offence:

(a) to take, or permit to be taken, an indecent photograph of a child (a person under the age of 16); or
(b) to distribute or show such indecent photographs or pseudo-photographs; or
(c) to have in his possession such indecent photographs or pseudo-photographs with a view to their being distributed or shown by himself or others…

By virtue of the amendment made by the 1994 Act, the term *photograph* includes data stored on a computer disk or by other electronic means which are capable of conversion into a photograph, including graphic images (Section 7.4(b)). The test, therefore, is that if data can be converted into an indecent image it will be deemed a photograph for the purposes of the section. In addition, Section 160 of the English Criminal Justice Act, 1988 provides inter alia that:

1 It is an offence for a person to have any indecent photograph or pseudo-photograph of a child in his possession.
2 Where a person is charged with an offence under subsection (1) it shall be a defense for him to prove -
  (a) that he had a legitimate reason for having the photograph or pseudo-photograph in his possession; or
  (b) that he had not himself seen the photograph or pseudo-photograph and did not know nor had any cause to suspect, it to be indecent; or
  (c) that the photograph or pseudo-photograph was sent to him without any prior request made by him or on his behalf and that he did not keep it for any unreasonable time.

The Court of Appeal case of R. v. Fellows, Arnold ([1997] 2 All E.R. 548) is a leading English case on the interpretation of Section 1 of the Protection of Children Act, 1978, and specifically on the question of what might constitute the "distributing" or "showing" of offending material.

> CASE EXAMPLE (R. v. FELLOWS 1997):
> Alban Fellows and Stephen Arnold were arrested after a large amount of child pornography was found on an external hard drive attached to a computer belonging to Fellows' employer, Birmingham University. Fellows and Arnold were convicted of distributing the child pornography in this archive to others on the Internet. In appeal, defense counsel submitted to the court, *inter alia*, that the data was not "distributed or shown" merely by reason of its being made available for downloading by other computer users, since the recipient did not view the material held in the archive file, but rather a reproduction of that data which was then held in the recipient's computer after transmission had taken place. The Court of Appeal rejected this argument, holding at p. 558 that:
>
> the fact that the recipient obtains an exact reproduction of the photograph contained in the archive in digital form does not mean, in our judgment, that the (copy) photographs in the archive are not held in the first appellant's possession with a view to those same photographs being shown to others. The same data are transmitted to the recipient so that he shall see the same visual reproduction as is available to the sender whenever he has access to the archive himself.
>
> Fellows was sentenced to three years in prison and Arnold to six months.

In another English case, R. v. Bowden ([2000] 1 Crim.App.R. 438), the Court of Appeal considered the question of whether the downloading and/or printing out of computer data of

indecent images of children from the Internet was capable of amounting to the offence of making child pornography.

> CASE EXAMPLE (R. v. BOWDEN 2000): Downloading and printing images amounts to 'making' and not mere 'possession'.
> The facts of the case as set out in the judgment of Otton L.J. are that the defendant took his computer hard drive in for repair. While examining the computer, the repairer found indecent material on the hard drive. As a result of a subsequent investigation, police seized a computer and equipment including hard disk and floppy disks from the defendant. They examined the disks, which contained indecent images of young boys. The defendant had downloaded the photographs from the Internet, and either printed them out himself, or stored them on his computer disks. It was not contested that all the photographs were indecent and involved children under sixteen years. When arrested and interviewed, the defendant accepted that he had obtained the indecent material from the Internet and downloaded it onto his hard disk in his computer for his own personal use. He did not know it was illegal to do this. He admitted that he had printed out photographs from the images he had downloaded.
>
> At first instance, defense counsel submitted that the defendant was not guilty of "making" photographs contrary to the section. He submitted that the defendant was in possession of them but nothing more. The Court of Appeal held that despite the fact that he made the photographs and the pseudo-photographs for his "own use", the defendant's conduct was clearly caught by the Act, stating at p. 444:
>
> Section 1 is clear and unambiguous in its true construction. Quite simply, it renders unlawful the making of a photograph or a pseudo-photograph… the words "to make" must be given their natural and ordinary meaning… As a matter of construction such a meaning applies not only to original photographs but, by virtue of section 7, also to negatives, copies of photographs and data stored on computer disk". The court adopted the prosecution's submissions, reported at pp. 444 to 445 of the judgment that: "a person who either downloads images onto a disk or who prints them off is making them. The Act is not only concerned with the original creation of images, but also their proliferation. Photographs or pseudo-photographs found on the Internet may have originated from outside the United Kingdom; to download or print within the jurisdiction is to create new material which hitherto may not have existed therein.

By equating downloading a file from the Internet with making it, the court concluded that Bowden had violated Section 1(1) (a) of the Protection of Children Act 1978.

> CASE EXAMPLE: Atkins [2000] 1 W.L.R. 1427 – knowledge is an essential element of the offence of possessing an indecent image of a child.
> This case came to the High Court by way of case stated. The questions for the opinion of the High Court were: (i) in respect of a charge of possession of an indecent photograph of a child under section 160(1) of the Act of 1988, was the magistrate right to hold that it was an offence of strict liability, mitigated only by the three statutory defenses in subsections 2(a), (b) and (c); (ii) in respect of the defense of legitimate reason under section 160(2)(a) of the Act of 1988, was the magistrate right to hold that the defense was limited to specified anti-pornographic campaigners, defined medical researchers and those within the criminal justice system, namely magistrates, judges, jurors, lawyers and forensic psychiatrists whose duties in the enforcement of the law necessitated the handling of the material in each particular case, and that the defense was not capable of including research into child pornography even if "honest and straightforward"; (iii) in

respect of a charge of making an indecent photograph of a child under section 1(1)(a) of the Act of 1978, was the magistrate right to hold that it required some act of manufacture, namely, "creation, innovation or fabrication" and that making did not mean "stored, isolated or reserved in whatever form", or copying an image or document whether knowingly or not.

The court held:

(1) That whether the defense of "legitimate reason" was made out was a question of fact: where academic research was put forward as a legitimate reason, the question was whether the defendant was a genuine researcher with no alternative but to have indecent photographs in his possession. The courts were entitled to be skeptical and should not too readily conclude that the defense had been made out.

(2) That "making" included the intentional copying or storing of an image or document on a computer: the defendant should have been convicted of making the pictures which he deliberately saved, but was not guilty of making the pictures which the computer had automatically saved without his knowledge.

(3) That knowledge was an essential element of the offence of possessing an indecent photograph of a child: a defendant could not be guilty of the offence unless he knew that he had photographs in his possession, or knew that he once had them in his possession, or knew that he possessed something with contents which in fact were indecent photographs. Since the defendant was unaware of the existence of the cache which contained the unsaved photographs, he was not guilty of possessing those photographs.

(4) That an item consisting of parts of two different photographs taped together could not be said to be an image which appeared to be a photograph: a photocopy of such an item might constitute a pseudo-photograph.

CASE EXAMPLE: Dooley [2006] 1 WLR 775: possession of indecent images in a shared folder may amount to the offence of possession with a view to distribution if the accused has the requisite intention to allow others access to the images.

The defendant's computer was found to contain thousands of indecent images of children. Most had been downloaded via an Internet file-sharing system whereby members installed software allowing files, held in their shared folder, to be accessed and downloaded directly into share folders of other members whilst connected to the Internet. The defendant pleaded guilty to counts of possession of and making indecent photographs.

He was further charged with counts of possession with a view to distribution in respect of six files downloaded which were found in his shared folder. The defendant claimed that he did not have the intention to distribute or show these photographs. He normally moved files from the shared folder to a folder not accessible to other members but had not yet moved those particular files because of the process he used to download and move images in bulk. The trial judge made a preliminary ruling that if the defendant had knowledge that photographs he downloaded were likely to be seen by others having access to the shared folder, then he possessed them "with a view to" their being distributed or shown contrary to s. 1(1)(c) of the 1978 Act. As a result of that ruling, the defendant pleaded guilty and was convicted. On appeal on that point, the Court of Appeal, finding that the defendant did not have the necessary intention to allow the conviction to stand, allowed the appeal, holding that the question which the jury would have to resolve was whether at least one of the reasons why the defendant left the images in the shared folder was so that others could have access to the images in it. If they so

found, the defendant would be guilty of possession with a view to showing or distributing the images. As the defendant was convicted on the basis of the trial judge's erroneous ruling, the conviction was quashed.

CASE EXAMPLE: Porter [2006] 1 WLR 2633 – 'possession' requires an element of custody and control: deleted images which the accused could no longer retrieve were not held to be in his possession. Custody and control was a question of fact for a jury to decide.

Police raided the defendant's home and seized two computers, the hard drives of which contained files with indecent images of children. The defendant was charged with two counts of possession contrary to section 160(1) of the 1988 Act. The first count related to still images and the second count to movie files. The date of possession charged was the date of the raid by the police.

The following facts were stated by the court at paragraphs 4 to 6 of the judgment:

- Of the 3,575 still images, two were found in [the first computer] and the remaining 3,573 in [the second computer]. The two still images found in [the first computer] and 873 of the remaining 3,573 found in [the second computer] had been deleted in the sense that they had been placed in the recycle bin of the computer which had then been emptied. The remaining 2,700 still images were saved in a database of a program called ACDSee. This program is designed for viewing graphical images and is used by photographers. ~When opened into eh "gallery view", the program creates "thumbnail" images of ht pictures viewed. These would originally have been larger images associated with each thumbnail. If one had clicked on the thumbnail, the larger image could have been viewed. All of the larger images had, however, been deleted. The effect of deleting the larger images was that the thumbnail could no longer be viewed in the gallery view. But a trace of each thumbnail ("the metadata") remained in the database of the program.
- Of the 40 movie files, seven were recovered from [the first computer]. All of these had been placed in the recycle bin which had then been emptied. The remaining 33 files were recovered from [the second computer]: they had not been saved, but were recovered from the cache (temporary internet files) record of the two hard disk drives.
- It was conceded by the Crown [prosecution] that: (i) all the deleted items had been deleted before [the date of the raid by the police]; (ii) the defendant did not have the software to retrieve or view the deleted still or movie files; and (iii) the thumbnail images were only retrievable with the use of specialist forensic techniques and equipment provided by the United States Federal Government which would not have been available to the public. It is common ground that the defendant could have acquired software to enable him to retrieve the items which had been emptied from the recycle bin. Such software could have been downloaded from the Internet or otherwise purchased. There was no evidence that the defendant had attempted to do this.

The Court of Appeal held, allowing the appeal, (as reported in the WLR headnote) that "the interpretation adopted by the judge that images were in a person's possession even if they could not be retrieved, could give rise to unreasonableness and was not compelled by either the express words of the statute or by necessary implication; that the concept of having custody and control of the images should be imported into the definition; that in the case of deleted computer images, if a person could not retrieve or gain access to an image, he had put it beyond his reach and no longer had custody or control of it; that it

was a matter for the jury to decide whether the images were beyond the control of the defendant having regard to all the factors of the case, including the defendant's skill in the use of computers; that the judge was right not to withdraw the counts from the jury, but that he had failed to direct the jury about the factual state of affairs necessary to constitute possession, nor had he directed them that the mental element of the offence required proof that the defendant did not believe that, at the material time, the images were beyond his control; and that, accordingly, the convictions for the offences contrary to section 160(1) of the 1978 Act would be quashed."

In recognition of the growing problem, penalties for computer-related crimes are being made more severe. For instance, the English Criminal Justice and Court Services Act, 2000 increased the maximum penalty for offences contrary to Section 1 (1) of the Protection of Children Act, 1978 from 3 to 10 years imprisonment. Anyone convicted of or pleading guilty to an offence involving child pornography might be subject to a range of other legal consequences including registration under the Sex Offenders Act, 1997, disqualification from working with children under the Criminal Justice and Court Services Act, 2000 and being barred or restricted from employment as a teacher or worker with persons under the age of 19.

The English Sentencing Advisory Panel (SAP) is a body established to advise the Court of Appeal. In August 2002, it published its advice on offences involving child pornography. (See Gillespie, Alisdair A. "Sentences for Offences Involving Child Pornography," [2003] Crim.L.R. 81.)

The SAP's advice was discussed in the case of R. v. Oliver, Hartrey and Baldwin [2003] Crim.L.R. 127 where the English Court of Appeal dealt with three appeals together for the purpose of giving sentencing guidelines for offences involving indecent photographs and pseudo-photographs of children. The court agreed with the panel that the two primary factors which determined the seriousness of a particular offence were the nature of the indecent material and the extent of the offender's involvement with it. The seriousness of an individual offence increased with the offender's proximity to and responsibility for the original abuse. Any element of commercial gain would place an offence at a high level of seriousness. Swapping of images could properly be regarded as a commercial activity, albeit without financial gain, because it fuelled demand for such material. Widespread distribution was intrinsically more harmful than a transaction limited to two or three individuals. Merely locating an image on the Internet would generally be less serious than downloading it. Downloading would generally be less serious than taking an original photograph. Possession, including downloading, of artificially created pseudo-photographs and the making of such images should generally be treated as being at a lower level of seriousness than the making and possessing of images of real children. The court noted, however, that although pseudo-photographs lacked the historical element of likely corruption of real children depicted in photographs, pseudo-photographs might be as likely as real photographs to fall into the hands of or to be shown to the vulnerable, and therefore to have an equally corrupting effect.

The SAP categorized the increasing seriousness of material into five levels, characterized by the court, in making certain amendments, as follows:

1 images depicting erotic posing with no sexual activity;
2 sexual activity between children or solo masturbation by a child;
3 non-penetrative sexual activity between adults and children;
4 penetrative sexual activity between adults and children;

5 sadism or bestiality.

The court held that a fine would normally be appropriate in a case where (i) the offender was merely in possession of material solely for his own use, including cases where material was downloaded from the Internet but was not further distributed, (ii) the material consisted entirely of pseudo-photographs, the making of which had involved no abuse or exploitation of children, or (iii) there was no more than a small quantity of material at level 1.

The court agreed with the SAP's recommendation that in any case which was close to the custody threshold, the offender's suitability for treatment should be assessed with a view to imposing a community rehabilitation order with a requirement to attend a sex offender treatment program.

With regard to custodial sentences, in summary, the court found as follows:

- a sentence of up to six months would be appropriate in a case where the offender was in possession of a large amount of material at level 2 or a small amount at level 3 or the offender had shown, distributed or exchanged indecent material at level 1 or 2 on a limited scale and without financial gain;
- a sentence of between six and twelve months would be appropriate for showing or distributing a large number of images at level 2 or 3 or possessing a small number of images at level 4 or 5;
- a sentence between twelve months and three years would be appropriate for possessing a large quantity of material at level 4 or 5, showing or distributing a large number of images at level 3 or producing or trading in material at level 1, 2 or 3;
- sentences longer than three years should be reserved for cases where images at level 4 or 5 had been shown or distributed, the offender was actively involved in the production of images at level 4 or 5, especially where that involvement included breach of trust and whether or not there was an element of commercial gain, or the offender had commissioned or encouraged the production of such images;
- sentences approaching the ten year maximum would be appropriate in very serious cases where the defendant had a previous conviction either for dealing in child pornography or for abusing children sexually or with violence.

The court set out specific factors which were capable of aggravating the seriousness of a particular offence:

1 the images had been shown or distributed to a child;
2 there were a large number of images;
3 the way in which a collection of images was organized on a computer might indicate a more or less sophisticated approach on the part of the offender to, say, trading;
4 images posted on a public area of the Internet;
5 if the offender was responsible for the original production of the images, especially if the child or children were family members or located through abuse of the offender's position of trust, for example, as a teacher;
6 the age of the children involved.

So far as mitigation was concerned, the court agreed with the SAP that some weight might be attached to good character, but not much. A plea of guilty was a statutory mitigating factor; the extent of the sentencing discount to be allowed for a plea of guilty would vary according to the timing and circumstances of the plea.

Applying these principles to the instant cases, the court imposed a sentence of 8 months imprisonment with an extension of 28 months in the case of a man of previous good character

who had pleaded guilty to six offences of making indecent photographs or pseudo-photographs of a child, his computer and some floppy disks having been found to contain some 20,000 images at levels 3 and 4. The court imposed a sentence of three years on a guilty plea in the case of a man who had distributed and made photographs of children at level 4, his computer systems having been found to contain a total of 20,000 indecent images and 500 movie files of child abuse. In the third case, the court imposed a sentence of 2.5 years for the offences of making indecent photographs. A concurrent sentence of 3 years was imposed for indecent assault on a girl aged 8 or 9 years, a video recording depicting the defendant committing the assault having been found in the home of another person.

Child prostitution and pornography are scheduled offences to the English Serious Crime Act 2007 which enables the court (on conviction on indictment) to impose a serious crime prevention order. (See also, Terrell [2008] 2 All ER 1065: imprisonment for public protection order.)

In Ireland, production, distribution and possession of child pornography are prohibited by the Child Trafficking and Pornography Act 1998. Definitions of visual and audio representation and document are careful to include any computer disk or other thing on which data capable of conversion into any such document is stored, and a visual representation of child pornography is expressly defined to include reference to a figure resembling a person that has been generated or modified by computer-graphics or otherwise, and in such a case the fact, if it is a fact, that some of the principal characteristics shown are those of an adult shall be disregarded if the predominant impression conveyed is that the figure shown is a child.

Any attempt at introducing sentencing guidelines into the Irish criminal process has been rejected. The overriding principle is articulated in The People (DPP) v McCormack [2000] 4 IR 356 at p. 359 in which it was held that:

> "Each case must depend upon its special circumstances. The appropriate sentence depends not only upon its own facts but also upon the personal circumstances of the accused. The sentence to be imposed is not the appropriate sentence for the crime, but the appropriate sentence for the crime because it has been committed by that accused."

Thus sentencing discretion remains with the trial judge (or sentencing judge on a plea of guilty) subject to a right of appeal by the accused as to severity of sentence and by the prosecution as to undue leniency of sentence. The general approach to sentencing is that a notional sentence is arrived at (having regard to the maximum penalty but not using it as a starting point) by the judge assessing where the particular offence lies on the overall scale of gravity. Aggravating factors are considered and credit is then given for mitigating factors – the overall goal is to arrive at a sentence that is fair and proportionate.

In the context of offences concerning child pornography, the general aggravating factors identified in R. v. Oliver [2003] 2 Cr.App. R.(S.) 15 are applicable to Irish law. General mitigating factors apply such as a plea of guilty (the earlier in the process the better), a lack of previous convictions and cooperation with the police authorities in the investigation of the offence. In addition, efforts to seek professional help for treatment may be considered mitigating factors in some circumstances.
(See generally, O'Malley, Sentencing Law and Practice, second edition, Thomson Round Hall, 2006.)

> CASE EXAMPLE: DPP v Loving [2006] 3 IR 355 – the option of a suspended sentence (i.e. non-custodial) may be considered for a first offence, at the lower levels of

seriousness of possession, where there is no intention to distribute and the accused is cooperative: sentence reduced.

In this Irish case, the facts were that following a complaint alleging fraud, the gardaí obtained a search warrant to search the defendant's home. The defendant's computer and computer-related materials, including floppy discs were seized. Upon forensic examination, 175 discrete images of child pornography were found with a large amount of adult pornography. On being questioned by the gardaí, the defendant said that he had not originally been interested in child pornography but that pop-ups appeared and his curiosity got the better of him: he thought he was merely looking at advertisements for the particular sites but accepted he had got drawn into them over a couple of months and had saved them onto floppy discs. He pleaded guilty to a count of possession contrary to s. 6 and the sentencing court imposed a sentence of five years imprisonment (the maximum available), suspending the final two years. The defendant appealed the severity of the sentence imposed.

The Court of Criminal Appeal in its judgment considered R v Oliver [2003] 1 Cr App R 28 and the principles and categories of classification set out therein. The court stated:

> "The offence of possession of child pornography is comparatively new in our law. It is a response to the very serious evidence of gross and shocking child abuse that has emerged over recent decades. It also highlights the possibility of the abuse of the wonders of the internet to transmit degrading images of abuse of both adults and children. The legislature has chosen to criminalise activities concerning child pornography. It has been discovered that many individuals have a propensity to access and use images of child pornography. The task of the courts is, following the guidance given by the Oireachtas [the Irish Parliament], to measure the seriousness of individual cases and to fix appropriate penalties."

It held that the following principles should be taken into account in sentencing for this type of offence:

- the Act of 1998 distinguishes between cases of active use of child pornography involving either dissemination of images for commercial or other exploitative purposes (s. 5) and mere possession (s. 6);
- the offence of possession may be tried summarily with a maximum sentence of one year's imprisonment or on indictment with a maximum of five years;
- two of the basic mitigating factors in sentencing must be had regard to namely whether the accused has accepted responsibility including entering a guilty plea, and the accused's previous character, i.e., whether he has previous convictions for similar offences;
- it is necessary to consider the individual offence: how serious and numerous were the actual pornographic images?
- The circumstances and the duration of the activity leading to the possession of the images should be considered.

The Court of Criminal Appeal reduced the sentence to one year of imprisonment (which had already been served by the time the appeal came on for hearing), concluding:

> "Where the offence is at the lower levels of seriousness, there is no suggestion of sharing or distributing images, the accused is cooperative and it is a first offence, the option of a suspended sentence should at least be considered."

A "suspended sentence" is explained by O'Malley, Sentencing Law and Practice (2nd ed.), at p. 453 as follows:

> Suspension of sentence involves imposing a determinate prison sentence but suspending it on certain conditions, a common condition being that the offender enters into a bond to keep the peace and be of good behaviour for a defined period.

O'Malley refers to the oft quoted *dictum* of Bray C.J in Elliot v Harris (No. 2) (1976) 13 S.A.S.R. 516 at 517:

> "A suspended sentence is a sentence to imprisonment with all the consequences that such a sentence involves on the defendant's record and his future and it is one which can be called automatically into effect on the slightest breach of the term of the bond of its currency."

As such it has been described by one commentator as of the nature of a Damocles' Sword (Osborough (1982) 17 Ir. Jur. (n.s.) 221).

> CASE EXAMPLE: DPP v Smith [2008] IECCA 1 – where the commission of the offence involves an element of breach of trust, a custodial sentence is appropriate.
> In this Irish case, the accused pleaded guilty to possession of child pornography contrary to s. 6 of the 1998 Act. The police had recovered a collection of almost 15,000 images (built up over a period of some eight years) of children in various states of undress, including graphic sexual imagery and some children engaging in sexual acts. The sentencing judge imposed a three year term of imprisonment on the accused with two years of post-release supervision to follow.
> The accused appealed severity of sentence to the Court of Criminal Appeal arguing that a custodial sentence is not necessarily required for this kind of offence, notably where it is a first offence, and that a medical report, pointing in the direction of mitigation had not been taken into account by the sentencing court.
> The Court of Appeal agreed with the accused's submissions in respect of the medical evidence but was of the view that the sentencing judge was correct in imposing a custodial sentence having regard to the gravity of the offence. The court noted:
>
> > "What makes the offence more reprehensible is the fact that he used his employer's computer facilities to facilitate these activities and that in itself was a significant breach of trust."
>
> Sentence was reduced to eighteen months imprisonment.

> CASE EXAMPLE: DPP v Curtin – evidence found on the accused's computer was held to be inadmissible at his trial because the search warrant was a day out of date at the time of search.
> As a result of the uncovering of the notorious child pornography website, Landslide Productions Inc, in the U.S., synchronised raids were made at an international level on thousands of homes of those whose credit card details were found on the billing records of that website company. Among the homes searched in Ireland, under 'operation ameythst' was that of a sitting Circuit Court Judge. Police had obtained a search warrant on the 20th May 2002 pursuant to s. 7 of the Child Trafficking and Pornography Act 1998 which authorised them, *inter alia*, to enter 'within 7 days from the date of the warrant' the place named in the warrant. On the 27th May police gained entry into the Judge's home and seized a computer and disks alleged to contain visual images of children engaged in explicit sexual activity. The accused was charged with knowingly having in his possession child pornography at his home, on the 27 May, 2002, contrary to s. 6 of the 1998 Act. At his trial, a *voir dire* application (on a legal issue in the absence of the jury) was made on the admissibility of the evidence seized on foot of the warrant on the basis that the warrant had expired at midnight the night before the police gained entry to

the accused's home. Under the Irish Constitution, 'the dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law' (Article 40.5). The trial judge ruled that the search warrant was spent at the time the accused's home was entered and searched. He held that there was a violation of the accused's constitutional rights and accordingly evidence obtained in the course of the search would not be admissible in the case against him. The trial judge directed the jury to acquit the accused.

The ruling threw the State into a political and constitutional crisis. A sitting judge had never been removed from office in the history of the State: the grounds for same lie in Article 35.4.1 of the Constitution which permit the Houses of Parliament (the Oireachtas) to pass a resolution calling for the removal of a judge for 'stated misbehaviour or incapacity'. The concern was that attempting to remove him from office on the basis of illegally obtained evidence would infringe his right to fair procedures. An Oireachtas committee was established following a proposal to remove him from office. The judge brought judicial review proceedings challenging a direction of that committee that he produce his computer for inspection and challenging the procedures of that committee. He maintained that the offending material was not knowingly in his possession. Following lengthy court hearings in the High Court and Supreme Court, the Judge's challenge was dismissed, and following unsuccessful attempts to stop the parliamentary inquiry on medical grounds, the Judge finally resigned from office.

Online grooming

In addition to the criminalisation of child pornography in the Cybercrime Convention, the Council of Europe's Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201) criminalises some other computer-related activities in the area of sexual abuse, including online grooming. Grooming consists of paedophiles establishing a trust relationship with a minor in order to subsequently meet for sexual abuse. Online grooming, i.e., using the Internet to establish trust, is criminalised by the Lanzarote Convention in Article 23:

> "the intentional proposal, through information and communication technologies, of an adult to meet a child (…) for the purpose of committing [a sexual offence], where this proposal has been followed by material acts leading to such a meeting".

The sexual offences at issue are having sex with a child under the legal age for sexual activities, and producing child pornography. In this provision, the preparatory act of arranging a meeting and, for example, booking a train ticket, constitutes a crime, regardless of whether the meeting actually takes place. Of course, a key issue is whether it can be proven that the meeting has the purpose of having sex or making (child-porn) images, which will require considerable circumstantial evidence.

In Dutch law, grooming was criminalised in January 2010. To implement the Lanzarote Convention, which the Netherlands signed in October 2007, a new provision, Article 248e, was added to the Dutch Criminal Code (*Staatsblad* 2009, 544). The provision is somewhat broader than the Lanzarote Convention, in that it criminalises using *a computer or* a communication service to propose a meeting with a minor under the age of 16 with the intention of sexual abuse or creating child pornography, if any act is performed to effectuate such a meeting. The maximum penalty is two years' imprisonment.

Online grooming is not yet a crime in Ireland, though again it is the subject of increased political debate, and the Joint Oireachtas [Irish house of parliament] Committee on Child Protection recommended in November 2006, the introduction of a criminal offence for grooming a child for sexual abuse. The offence would cover acts preparatory to or intended to facilitate the sexual

abuse of a child at a later date – including arranging to meet a child for that purpose or showing a child pornographic material.

The UK introduced a specific offence to tackle the threat of child grooming, particularly in respect of those who seek to use the internet to solicit children for abuse, in the Sexual Offences Act 1993, s. 15 (amended by s. 73(a) of the Criminal Justice and Immigration Act 2008). The offence is not technology-specific.

> "15(1) A person aged 18 or over (A) commits an offence if-
> (a) A has met or communicated with another person (B) on at least two occasions and subsequently–
> (i) A intentionally meets B,
> (ii) A travels with the intention of meeting B in any part of the world or arranges to meet B in any part of the world, or
> (iii) B travels with the intention of meeting A in any part of the world,
> (b) A intends to do anything to or in respect of B, during or after the meeting mentioned in paragraph (a)(i) to (iii) and in any part of the world, which if done will involve the commission by A of a relevant offence,
> (c) B is under 16, and
> (d) A does not reasonably believe that B is 16 or over."

The maximum penalty for conviction on indictment is 10 years imprisonment.
The actus reus requires that there has been at least two communications: this ought to cover individual emails and text messages, but is designed to stop the law being applied to single acts. There is no requirement for the communication to be sexual.
An article written by one of the members of the Home Secretary's Internet Task Force on Child Protection, Alisdair A. Gillespie, involved in drafting the legislation, is instructive (Tackling Child Grooming on the Internet: The UK Approach, The Bar Review, February 2005). In relation to actus reus he states:

> "The crux of [section 15] is the meeting. Grooming (…) is very transient behaviour and it is virtually impossible to define precisely what behaviour amounts to grooming, or, indeed, when it starts or finishes. It is important to note, therefore, that although this provision is frequently referred to as the 'grooming offence' its actual description is 'meeting a child following grooming etc.' Whilst the inclusion of the word 'etc.' is somewhat unhelpful, it does reinforce the fact that this offence is dealing with the *effects* of grooming and not the grooming itself. The Task Force decided that the mischief we were trying to prevent was those people meeting children they have groomed over the Internet so that they can abuse them. The meeting became the step at which we believed criminal liability could accrue although through the use of the Criminal Attempts At 1981, it would also be possible for someone who attempted to meet with a child in these circumstances too. The addition of the alternative actus reus of travelling to meet the child was added because it was felt that this was still proximate enough (with the requisite mens rea) but would also ensure that the police did not have to risk the safety of a child by, in effect, observing an actual meet, something that could not be justified as the risk to the child would be too great."

In the same article, in relation to the mens rea of the section 15 offence Gillespie states the following:

"(…) it is likely that there will be a considerable number of ways of proving intent. The content of the communications are likely to be of assistance, especially as … in many situations the content of such material is likely to be sexual. The police are already used to the concept of forensically examining computers to recover emails and other computer data, and this is likely to fine relevant material. It is important to note that in the grooming context, there will be at least two opportunities to gather such evidence, because not only will it be the offender's computer that could contain information but also the child's. Other computer data that might be of assistance is between the offenders and others."

Racism

The Additional Protocol to the Convention on Cybercrime was agreed by the member states for the purpose of supplementing the provisions of the Cybercrime Convention as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

"Racist and xenophobic material" is defined in Article 2 as any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

The Additional Protocol requires parties to take measures at national level to establish as criminal offences the following conduct:

1. dissemination of racist and xenophobic material through computer systems (Article 3);
2. racist and xenophobic motivated threat, being threatening certain classes of person or persons (as per the Article 2 definition) through a computer system with the commission of a serious criminal offence (Article 4);
3. racist and xenophobic motivated insult, being insulting publicly certain classes of person or persons through a computer system (Article 5);
4. denial, gross minimisation, approval or justification of genocide or crimes against humanity, being the distribution or otherwise making available to the public through a computer system, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law (Article 6).

The connecting clause (Article 8) declares several provisions from the Cybercrime Convention, such as definitions and liability of legal persons, to be *mutatis mutandis* applicable. Provisions on aiding and abetting, however, are separately included in the Protocol (Article 7), excluding, for example, criminal attempt from the scope of the Protocol, in contrast to Article 11(2) of the Convention.

The Netherlands is ratifying the Protocol; a Bill to that effect was pending in the First Chamber in early 2010. The acts covered by the Protocol, however, are already criminal under existing legislation, since the provisions on racism do not refer to media and hence are applicable as well in an online context. Article 137c DCC penalises insult of communities, i.e., utterances in public – orally, in writing or images – that are intentionally insulting to groups of the population on the basis of their race, religion, philosophy of life, sexual orientation or handicap. Article 137d similarly penalises discrimination or inciting hatred of people on these grounds. Both offences are punishable by a maximum imprisonment of one year, or, if done by profession or custom or in alliance with others, two years. Article 137e criminalises the publication of discriminatory statements as well as dissemination or stocking for dissemination purposes of carriers with

discriminatory utterances, if done otherwise than for the purposes of professional reporting. This offence is punishable with a maximum of six months' imprisonment, or, if done by profession of custom or in alliance with others, one year imprisonment. Finally, participating in or supporting discriminatory activities is punishable on the basis of Article 137f DCC with maximally three months' imprisonment, and discriminating people in the performance of a profession or business is punishable with six months' imprisonment (Article 137g DCC).

> CASE EXAMPLE: discrimination of Jews
> The Appeal Court Amsterdam (17 November 2006, LJN AZ3011) convicted a defendant for publishing discriminatory statements about Jews and homosexuals on a website. The publication of statements like "yet another of those daylight-shirking lawless Jews" and "so even today Jews still act like beasts" were unnecessarily offending. The Court considered the Internet to be a wonderful means for exercising freedom of expression, but reasoned that there are limits to what is acceptable for publication on the Internet, given that anyone can publish, without any obstacle, texts that are hurting and offending to others while such publication does not serve any respectable aim. The defendant's argument that the website was a "mildly provocative, amusingly stinging" means of attracting readers' attention to his column about Mel Gibson's *The Passion of Christ* was rejected; the court reasoned that the debate could equally well be conducted without the grievous passages. Hence, the defendant was convicted to a fine of 500 Euros and a suspended sentence of one week's imprisonment with two years' probation.

The only provision from the Protocol that is not as such criminalised in the Netherlands, is Article 6, concerning genocide denial. Often, genocide denial will be punishable on the basis of Article 137c, 137d, or 137e DCC, since these statements will generally be insulting or discriminatory for the groups subjected to the genocide or crimes against humanity. To make genocide denial more visibly punishable, a Bill has been proposed to criminalise 'negationism' in a new provision, Article 137da DCC (Bill No. 30579), which would fully cover the acts mentioned in Article 6 of the Protocol. This Bill, which was introduced in June 2006, is still being discussed in the Second Chamber as of March 2010. In the meantime, the legislator has chosen to ratify the Protocol while making a reservation for Article 6, criminalising genocide denial only when it incites hatred, discrimination, or violence against individuals or groups based on race, colour, ethnic background, or religion (i.e., the crimes already covered in Articles 137c, 137d, or 137e DCC).

> CASE EXAMPLE: Holocaust denial
> A defendant was accused of discrimination for publishing on the Internet a website in Dutch with a text titled "The Holocaust that never was". The text included statements like "the lie of the century" and "all stories about the Holocaust have been invented for the purposes of the own profit of Zionist Jews", linked to, inter alia, Richard E. Harwood's *Did Six Million Really Die*, and included Dutch translations of several chapters of this book. Referring to Article 10(2) ECHR, the District Court 's-Hertogenbosch (21 December 2004, LJN AR7891) considered the text to cross the limits of lawful freedom of expression and to constitute the publicly intentional insulting, in writing, of a group of people based on their race and/or religion (Article 137c DCC). Considering as mitigating circumstances that the defendant had not previously been convicted and that he had removed the webpage after notification by the police, the Court sentenced the defendant to a suspended sentence of four weeks' imprisonment with two years probation.

The United Kingdom and Ireland have yet to sign and ratify the Protocol on racism. In the UK Public Order Act 1986, "racial hatred" is defined in section 17 as meaning "hatred against a

group of persons in Great Britain defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins". By section 18(1) of that Act,

> "A person who uses threatening, abusive or insulting words or behaviour, or displays any written material which is threatening, abusive or insulting, is guilty of an offence if—
>
> (a) he intends thereby to stir up racial hatred, or
>
> (b) having regard to all the circumstances racial hatred is likely to be stirred up thereby."

Further offences under the Act include publishing or distributing written material which is threatening, abusive or insulting with the intent to stir up racial hatred or where the likelihood is that racial hatred will be stirred up having regard to the circumstances (s. 19) – this offence does extend to online publication or distribution as can be seen from the case example below – and possession of racially inflammatory material with a view to broadcasting or distributing it (s. 23). The Racial and Religious Hatred Act 2006 inserted a new part into the Public Order Act 1986 which provides for offences involving "religious hatred", in similar terms. The maximum sentence on a conviction on indictment is 7 years. Freedom of expression is expressly protected by section 27J which provides:

> "Nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult or abuse of particular religious or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytising or urging adherents of a different religion or belief system to cease practising their religion or belief system."

The Act allows for a defence where the accused proves that he was inside a dwelling and had no reason to believe that the words or behaviour used, or the written material displayed, would be heard or seen by a person outside that or any other dwelling. Hatred on the grounds of sexual orientation was included as a ground of offence into Part 3A by the Criminal Justice and Immigration Act 2008.

> CASE EXAMPLE: Sheppard and Whittle (2009) – inciting racial hatred online.
> The accused were charged under the Public Order Act with publishing racially inflammatory material, distributing racially inflammatory material and possessing racially inflammatory material with a view to distribution, before the Crown Court at Leeds. Evidence was given by the prosecution that the accused had published grotesque images of murdered Jewish people together with articles and cartoons ridiculing other ethnic groups. The investigation began when a complaint about a leaflet called Tales of the Holohoax was reported to the police in 2004. It was traced to a post office box registered in Hull, and police later found a website featuring racially inflammatory material. During an earlier trial in 2008 the accused skipped bail and fled to California where they sought asylum for persecution based on political beliefs. The Californian authorities refused to grant asylum to the accused and they were deported back to England to face trial. In what is reported as being the first conviction under the Act for inciting racial hatred online (see *www.guardian.co.uk* report of 10 July, 2009), Sheppard was found guilty on 16 charges and sentenced to four years and ten months imprisonment; Whittle was sentenced to two years and four months imprisonment having been found guilty of five offences.
> The case against Sheppard is under appeal before the Court of Appeal (as of November, 2009). He is attempting to make out a freedom of expression-based defence, arguing that the articles were posted on a website in California where they were lawful and enjoyed constitutional protection under the laws of the United States.

In Ireland, criminalisation of acts of a racist or xenophobic nature is limited to provisions set out in the Incitement to Hatred Act 1989. This Act sets out the three main offences of

- actions likely to stir up hatred (publish or distribute written material or use words, behave or display written material which is threatening abusive or insulting and intended, or having regard to all the circumstances, likely to stir up hatred) (s. 2);
- broadcast likely to stir up hatred (s. 3);
- preparation and possession of material likely to stir up hatred (s. 4).

The maximum penalty on conviction on indictment is two years imprisonment. Broadcasts would appear to include websites and online publication although computer use is not explicit in the Act. The Act is felt to fall short of necessary standards by commentators (see, for example, the Review/Submission by the National Consultative Committee on Racism and Interculturalism (NCCRI) of August 2001) on the basis that the offences, rather than relying on actual harm use the language of intention thereby allowing as a defence lack of intention to stir up hatred in conjunction with other defences. In addition, while the Act clearly defines such terms as "Broadcast", "Recording" and "Hatred" (hatred against a group of persons in the State or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation) it fails to define what exactly constitutes "incitement".

OTHER OFFENSES

Copyright infringement

Art. 10 of the Convention provides that parties should criminalise infringements of copyright and related rights when committed 'wilfully, on a commercial scale and by means of a computer system'. Parties can, however, refrain from establishing criminal liability if other effective remedies are available, and insofar as this does not derogate from parties' obligations under the relevant international treaties (Bern, Rome, TRIPs, WIPO) (art. 10(3) Convention).
Clearly copyright protection is very much a technology-related issue with global implications, particularly given the explosion onto the scene of Internet downloads, MP3 players, peer-to-peer programs and websites enabling, in particular, the availability of music, film and games. A thorough investigation of copyright and intellectual property law is beyond the scope of this chapter, but it would be remiss of us not to briefly touch upon the subject.

In Dutch law, copyright law is usually enforced by private law, but the Copyright Act (*Auteurswet*) contains several criminal provisions. Article 31 of the Copyright Act criminalises intentional infringement of someone else's copyright, punishable with a maximum imprisonment of six months. Intentionally offering for dissemination, stocking for multiplication or dissemination, importing or exporting, or keeping for pursuit of gain of an object containing a copyright infringement is punishable with maximally one year imprisonment (Article 31a Copyright Act), which rises to four years' imprisonment if done as a profession or business (Article 31b). Articles 34 through 35d contain further offences, the most important of which is the intentional altering copyrighted works in a way that is potentially harmful to their maker (Article 34).
For cybercrime purposes, Article 32a Copyright Act is particularly relevant. This provision criminalises misuse of devices, without consent, for circumventing copyright-protection measures that protect software. This offence, punishable with up to six months' imprisonment, was introduced to comply with the Software Directive, 91/250/EEC (1991). In contrast to the misuse of devices of Article 6 Cybercrime Convention, Article 32a only concerns devices *exclusively* (rather than primarily) targeted at software-protection circumvention.
The Copyright Directive 2001/29/EC contains a provision more similar to Article 6 Cybercrime Convention, in that it declares unlawful misuse of devices primarily targeted at circumventing copyright-protection measures of copyrighted works. This provision has been implemented in

Dutch private law rather than criminal law: Article 29a defines as tort the intentional circumvention of effective technical measures (paragraph 2) and the misuse of devices primarily designed to circumvent effective technical measures (paragraph 3(c)).

In Irish and English/Welsh legislation, copyright and related rights are enforceable using civil remedies, and by the prosecution of criminal offences. Thus, the principal Irish Act, the Copyright and Related Rights Act 2000 (as amended) provides in section 127 that infringement of the copyright in a work is actionable by the copyright owner; the civil reliefs available to the copyright owner include injunctive relief, account of profits and award of such damages as the court, in all the circumstances of the case, thinks proper, extending from compensatory damages to aggravated or exemplary damages. A defendant can rely on the defence that they did not know or had no reason to believe that copyright subsisted in the work to which the action relates, to resist the award of damages.

The Copyright and Related Rights Act 2000 (as amended) provides in section 140 a number of criminal offences. Section 140(1) provides:

> "A person who, without the consent of the copyright owner—
> (a) makes for sale, rental or loan,
> (b) sells, rents or lends, or offers or exposes for sale, rental or loan,
> (c) imports into the State, otherwise than for his or her private and domestic use,
> (d) in the course of a business, trade or profession, has in his or her possession, custody or control, or makes available to the public, or
> (e) otherwise than in the course of a business, trade or profession, makes available to the public to such an extent as to prejudice the interests of the owner of the copyright,
> a copy of a work which is, and which he or she knows or has reason to believe is, an infringing copy of the work, shall be guilty of an offence."

Further offences include:

- the making, selling, renting, lending, importing into the State or having in one's possession, custody or control an article designed or adapted for making copies of a work, knowing or having reason to believe that it has been or is to be used to make infringing copies (s. 140(3));
- the making, selling (etc.) of a protection-defeating device (s. 140(4)(a));
- the providing of information, or offering or performing any service, intended to make or assist a person to circumvent rights protection measures (s. 140(4)(b)).

These offences attract a maximum penalty on indictment of 5 years imprisonment and or a fine of up to €127,000. Emphasis is on possession for use for commercial gain rather than bare possession for the offences to be made out.

Similarly, in England and Wales, copyright and related rights may be enforced or protected in the civil and criminal sphere. There the principal legislation is the Copyright, Designs and Patent Act 1988 (as amended). Below is just one recent example of a case involving prosecution of copyright offences in the technology context. In the English/Welsh legislation, the protection of copyright material from devices and services designed to circumvent technological measures (implementing the EC Copyright Directive 2001/29/EC) comes under the realm of the criminal law.

> CASE EXAMPLE: Gilham [2009]
> The defendant was convicted of a number of offences arising from his commercial dealing in modification computer chips ("modchips"), which were alleged by the prosecution to be devices, "primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention" of effective technological measures within the

meaning of the Copyright, Designs and Patents Act 1988 as amended. The offences of which he was convicted included importing, advertising and offering for sale, selling and possessing such devices in the course of a business.
The modchips sold by the defendant were the Xecuter for use with the Microsoft Xbox, the ViperGC and Qoob chips for use with the Nintendo Gamecube and the Matrix Infinity for use with the Sony Playstation. The defendant sold the modchips either on their own, or already inserted into games consoles together with the paraphernalia needed to fit them. In some cases the purchaser of the modchip would have to download software from the Internet and install it in the modchip before it could be used. Once correctly installed, the modchips enable counterfeit games to be played on the consoles.
DVDs and CD-Roms on which games are sold for use with these game consoles contain substantial amounts of data in digital form. During the playing of a game, data is taken from the disk into the random access memory or RAM of the console. As the game is played, the data in RAM is over-written by different data from the disk. Precisely what data is taken from the disk into RAM will vary with the way the game is played, and cannot be predicted. At any one time only a very small percentage of the data on the disk is present in RAM.
The defendant appealed his conviction to the Court of Appeal.
In its judgment, the Court of Appeal identified the matters that the prosecution must prove for conviction on this type of offence:

(1) That the game is or includes copyright works within the meaning of section 1.
(2) That the playing of a counterfeit DVD on a game console involves the copying of a copyright work.
(3) That such copying is of the whole or a substantial part of a copyright work: section 16(3)(a).
(4) That the game consoles and/or genuine DVDs (i.e. copies of the copyright work or works created by or with the licence of the owner of the copyright) include effective technological measures within the meaning of section 296ZF designed to protect those copyright works.
(5) That in the course of a business the defendant sold or let for hire a device, product or component which was primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of those technological measures. It is to be noted that this issue does not depend on the intention of a defendant who is not responsible for the design, production or adaptation of the device, product or component: his intention is irrelevant.

The defendant argued on appeal that although there was copying, it did not represent at any one time the whole or substantial part of the games data on the DVD, and it followed that playing a counterfeit game dies not involve copying that infringes the rights of the copyright owner. The copy of the digital data is too short-lived to be regarded as tangible.
The Court rejected this argument. Noting that the legislation allowed for a situation where “Copying in relation to any description of work includes the making of copies which are transient or are incidental to some other use of the work” (s. 17(6)), the Court held that:

> “even if the contents of the RAM of a game console at any one time is not a substantial copy, the image displayed on screen is such. As we said in the course of argument, it may help to consider what is shown on screen if the "pause" button on a game console is pressed. There is then displayed a still image, a copy of an artistic work, generated by the digital data in RAM. The fact that players do

> not normally pause the game is immaterial, since it is sufficient that a transient copy is made."

Interestingly, the Court made the following remarks in conclusion on the question of the suitability of a jury trial for the determination of complex issues relating to interpretation and application of copyright-related matters:

> Lastly, we repeat with emphasis what Jacob LJ said in *Higgs* about the trial of cases involving recondite issues of copyright law before a jury. Cases that, for example, involve determination of difficult questions whether a copy is of a substantial part of a copyright work, can and should be tried in the Chancery Division before specialist judges. They can be so tried much more efficiently in terms of cost and time than before a jury, and questions of law can if necessary be determined on appeal on the basis of clear findings of fact. In appropriate cases, the Court will grant injunctive relief, and a breach of an injunction will lead to punishment for contempt of court. If the facts proven against a defendant show that he has substantially profited from criminal conduct, proceedings for the civil recovery of the proceeds of his crimes may be brought under Part 5 of the Proceeds of Crime Act 2002.

Cyberbullying

The Cybercrime Convention and other European instruments to regulate cybercrime are not exhaustive. The field of cybercrime continues to evolve, and new developments may show the need for adapting the law in addition to what international legal instruments so far require. One such development that has raised discussions is cyberbullying.

There is no specific legislation or case law in Dutch law on cyberbullying. Although cyberbullying is increasingly object of academic research, it has not so far been the subject of substantial public or policy debates in the Netherlands.

In Ireland, however, the issue of cyberbullying is increasingly becoming the subject of social and political debate, in particular in relation to the context of children and young people and therefore educational policy. The term is defined in an information booklet, A Guide to Cyberbullying (produced as a joint initiative between the Office for Internet Safety, the National Centre for Technology in Education, and children's charity Barnardos, 2008) as,

> "bullying which is carried out using the internet, mobile phone or other technological devices. Cyberbullying generally takes a psychological rather than physical form but is often part of a wider pattern of 'traditional bullying'. It can take the form of sending nasty, mean or threatening messages, emails, photos or video clips; silent phone calls; putting up nasty posts or pictures on a message board, website or chatroom; pretending to be someone else in a chatroom or message board or text message and saying hurtful things; or accessing someone's accounts to make trouble for them."

Bullying, this booklet states, is widely agreed to be behaviour that is sustained or repeated over time and which has a serious negative effect on the well-being of the victim and is generally a deliberate series of actions.

While the term cyberbullying is not used, the types of conduct described by the term do – at the serious end of the scale – come in under the harassment offence as provided for in section 10 of the Non-Fatal Offences Against the State Act 1997. That section makes it an offence "by any means including by use of the telephone" to harass another "by persistently following, watching, pestering, besetting or communicating with him or her". Harassment is defined in subsection (2):

> For the purposes of this section a person harasses another where—
> (*a*) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and
> (*b*) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.

The maximum penalty for conviction on indictment is 7 years imprisonment.

Below is a case example from England which related in part to the workplace (another area vulnerable to cyberbullying), and which combined anti-harassment legislation with the Computer Misuse Act.

> CASE EXAMPLE: Debnath [2005] The defendant was jailed for breaching a bail condition which prohibited her from accessing the Internet.
>
> This English case concerned harassment and misuse of a computer. It came before the Court of Appeal as an appeal against the wide terms of the restraining order made against the defendant as part of her sentence.
>
> The facts were that the defendant pleaded guilty to counts of harassment contrary to s. 2 of the Protection against Harassment Act 1997 and unauthorised modification of computer material contrary to s. 3 of the Computer Misuse Act 1991. She had had a 'one-night stand' with a work colleague and believed (wrongly) that she had caught a sexually transmitted disease from this encounter. This belief led her on a course of harassment of the complainant which included:
> - sending the complainant's fiancée emails purporting to be from one of his friends, informing her of alleged sexual indiscretions;
> - registering the complainant on a website called 'positive singles.com', a database for people with sexually transmitted diseases seeking sexual liaisons;
> - setting up a website called 'A is gay.com' which had a fake newspaper article detailing alleged homosexual practices by the complainant;
> - arranging to have the complainant receive large amounts of homosexual pornography;
> - arranging to have the complainant's email account sabotaged (paying a group of hackers to assist in the sabotage) so that he was unable to access his account and all mail went to another account to which the defendant had exclusive access.
>
> A condition of the defendant's bail was that she refrain from accessing the internet. She breached this condition and spent approximately six months in custody on remand. This time spent in custody was taken into account when the sentencing court sentenced her to a two-year community rehabilitation order and imposed a restraining order prohibiting her from (1) contacting directly or indirectly the complainant , his fiancée and others specified, and (2) publishing any information concerning the complainant and his fiancée, whether true or untrue, indefinitely.
>
> The defendant appealed the terms of the restraining order, citing Article 10 of the European Convention on Human Rights which provides:
>
> > "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (…).

> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

The court dismissed the appeal holding that the exceptional circumstances of the case justified the wide terms of the restraining order as necessary to prevent crime, prevent further harassment and protect the victims. The court cited with approval the test stated in Lester and Pannick, *Human Rights Law and Practice* (2nd ed.), p. 363:

> "Any restriction upon free speech must pass three distinct tests: (a) it must be prescribed by law; (b) it must further a legitimate aim; and (c) the interference must be shown to be necessary in a democratic society."

JURISDICTION

Jurisdiction in cybercrimes is a tricky issue. Acts on the Internet that are legal in the state where they are initiated may be illegal in other states, even though the act is not particularly targeted at that particular state. The cybercrime statutes that have been enacted over the past decades in numerous countries show varying and diverging jurisdiction clauses (for an overview, see Brenner & Koops 2004).

Jurisdiction has several forms: jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce. In this section, we focus on jurisdiction to prescribe: the authority of a sovereign "to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things (...) by legislation, by executive act or order, by administrative rule (...) or by determination of a court" (Restatement (Third) of Foreign Relations Law of the United States (1987), §401(a)).

Traditionally, jurisdiction is based primarily upon the concept of territory. 'Location' is therefore a primary constitutive factor for jurisdiction, even with cybercrimes. Countries can claim jurisdiction if the act of the cybercrime was committed on their territory, but also if the effect of the crime took place on their territory, or if the perpetrator resides in or happens to be found on their territory. There will be room for interpreting phrases such as "where the act takes place", which for cybercrimes might concern the keyboard where commands are entered into, a computer that stores or processes commands from the perpetrator, computers of victims entered by a hacker or a virus, and perhaps cables or other intermediary places of communication from perpetrators' to victims' computers.

Some countries even go so far as to claim jurisdiction on the basis of very indirect links with their territory. Malaysia has established jurisdiction in Article 9 of its Computer Crimes Act 1997 as follows: "this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time". Since most computers are actually connected, if only indirectly, through the Internet to Malaysia, this effectively gives Malaysia's cybercrime statute almost universal jurisdiction.

After territoriality, the nationality of the perpetrator is the second major constituting factor of jurisdiction in cybercrime: several countries claim jurisdiction if their nationals commit crimes outside their territory. Sometimes, besides nationality of the perpetrator, the nationality of the victim may also be a constituting factor.

The Cybercrime Convention uses location as the primary constituting factor of jurisdiction, but also nationality of the perpetrator. Article 22 reads as follows:

> "1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
>
> a in its territory; or
>
> b on board a ship flying the flag of that Party; or
>
> c on board an aircraft registered under the laws of that Party; or
>
> d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
>
> 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
>
> 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
>
> 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
>
> 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."

The last clause is particularly relevant for addressing jurisdiction conflicts. For the average cybercrime, the jurisdictional bases that countries use will often result in numerous potential claims for jurisdiction, based on the location of computers of perpetrator and victims as well as of intermediary computers. In those cases, it is important that states consult with each other to determine which state can best initiate criminal proceedings. Susan Brenner (2006) has helpfully provided a list of criteria that can help states in prioritising jurisdiction claims: place of commission, custody of the suspect, harm, nationality of victim and perpetrator, strength of the case against the defendant (including evidence and availability of witnesses and forensic experts for testimony), maximum punishment, fairness, and convenience.

Cooperation between States is key, to ensure that prosecutions are not defeated by jurisdictional issues. Legislative initiatives such as the European Arrest Warrant (European Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA)) provide a sound, operable procedure for enabling prosecutions of computer-related offences in the European State asserting jurisdiction. The underlying assumption of the European Arrest Warrant is that Member States trust the judicial systems in other Member States.

In the Netherlands, jurisdiction is set out first and foremost in Article 2 DCC, which provides that the Code "is applicable to anyone guilty of any offence in the Netherlands".

Article 4 DCC provides jurisdiction grounds for many specific offences committed outside of the Netherlands. The following cybercrimes are mentioned. Forgery, including computer forgery, committed abroad by Dutch government employees or employees of international organisations located in the Netherlands is punishable in the Netherlands, if the act is punishable in the country where it was committed (Article 4(11) *juncto* 225 DCC). The Netherlands also claims jurisdiction over computer sabotage or data damage committed against a Dutch national if the act is covered by article 2 of the International Convention for the Suppression of Terrorist Bombings (Article 4(13) DCC) or if it is covered by article 2 of the International Convention for the Suppression of the Financing of Terrorism (Article 4(14) *juncto* 161sexies and 350a DCC).

Article 5 DCC establishes jurisdiction on the basis of nationality of the perpetrator. With respect to cybercrimes, jurisdiction exists over the crime of publishing corporate secrets acquired by accessing a computer by a Dutch national (Article 5(1)(1) *juncto* 273 DCC), and over child pornography if committed by a Dutch national (Article 5(1)(3) *juncto* 240b DCC). Interestingly, jurisdiction in the latter case exists also if the person becomes a Dutch national only after the crime had been committed (Article 5(2) DCC). Moreover, jurisdiction also exists for child pornography committed not only by nationals, but also by foreigners with a fixed residence in the Netherlands, even when they come to reside in the Netherlands after the crime was committed (Article 5a DCC).
Finally, for a restricted number of crimes, countries may claim universal jurisdiction. The Netherlands claims universal jurisdiction over a number of crimes, such as attacks on the King and counterfeiting, but cybercrimes do not fall under any universal jurisdiction clause.

In Irish law dealing with computer crime, the question of jurisdiction is often integrated into the legislative section setting out the offence. Section 9 of the Criminal Justice (Theft and Fraud Offences) Act 2001 provides for the offence of dishonest use of a computer in the following terms:

> "A person who dishonestly, *whether within or outside the State*, operates or causes to be operated a computer *within the State* with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence." (Emphasis added.)

The offence of unauthorised access is laid down in section 5 of the Criminal Damage Act 1991 as follows:

> "A person who without lawful excuse operates a computer (…) *within the State with intent to access any data kept either within or outside the State*, or (…) *outside the State with intent to access any data kept within the State*, shall (…) be guilty of an offence." (Emphasis added.)

In both examples above, there has to be an Irish connection: in section 9, once the computer that is operated or caused to be operated is within the State the Irish courts have jurisdiction to try the offence; the location of the accused at the time of the commission of the offence is immaterial (but, as noted above, procedures such as use of the European Arrest Warrant, or extradition may have to be employed to bring the accused before the Irish courts if they committed the offence from a location outside the State). Section 5 includes a situation where the person is within the State at the time of the commission of the offence but gains unauthorised access to data located outside of the State. In such a situation, the Irish courts may try the accused, but may be called upon to cooperate with the State within whose jurisdiction the data was located.

In England, the Computer Misuse Act 1990 (as amended by the Police and Justice Act 2006), by sections 4 and 5, provides that liability for offences under the Act (ss. 1 to 3, see above) requires proof of at least one significant link with England (and Wales). This link would be satisfied where the accused was in England at the time of the commission of the offence in question, or where the targeted computer was situated in England.

It can be seen, therefore, that if a person within Ireland, without lawful excuse operated a computer with intent to access data held in a computer located in England, he would be guilty of an offence in both jurisdictions.

CONCLUSION

Cybercrime law is a continuously evolving process. In this Chapter, we have sketched an overview of cybercrime law in three European jurisdictions, England, Ireland, and the Netherlands. Our discussion of international legal instruments, both from the Council of Europe

and from the European Union, and national statutory law and case-law shows how complex and diverse the field of cybercrime law actually is. International instruments, in a response to the diverse legal computer-crime initiatives taken in European countries in the past, have aimed at approximating national laws. Although in many respects cybercrime law now shares a common international framework in which the major forms of cybercrime are criminalised, still national differences remain, not only in the details of criminalisation but also in the different emphasis put in legislation and case-law on various forms of cybercrime. This does not come as a suprise, nor should we worry about this. After all, criminal law needs to be effected and enforced in specific cases in local contexts, and so it is good that countries' efforts to combat cybercrime can evolve in ways that best fit their cultural traditions and legal systems. Still, when it comes to cybercrime with its intrinsic cross-border aspects, international efforts are vital to ensure that countries can offer expeditious mutual assistance and resolve jurisdiction conflicts when needed. The requirement of double criminality then implies that countries must stay up-to-date with criminalising new forms of cybercrime that are not covered by existing law. The Cybercrime Convention and its Additional Protocol will certainly not be the last efforts to approximate national laws in the cybercrime field, as the recent Lanzarote Convention also attests. We can look forward to an on-going interaction between national and international initiatives to keep our legal cybercrime frameworks up-to-date.

REFERENCES

Archbold, *Criminal Pleading, Evidence And Practice 2009*, Sweet & Maxwell Thomson Reuters.

Blackstone's *Criminal Practice 2009*, Oxford: Oxford University Press.

Brenner, S.W., 'The Next Step: Prioritizing Jurisdiction', in: Koops & Brenner (eds), *Cybercrime and Jurisdiction. A Global Survey*, The Hague: TMC Asser Press 2006, p. 327-349.

Brenner, S. and B.J. Koops, 'Approaches to Cybercrime Jurisdiction' (2004), 4 *Journal of High-Technology Law* (1), p. 1-46.

Cuijpers, C.M.K.C., 'Employer and Employee Power Dynamics. The division of power between employer and employee in case of Internet and e-mail monitoring and positioning of employees', (2007) 25 *The John Marshall Journal of Computer & Information Law* 37.

De Hert, P., G. González Fuster and B.J. Koops, 'Fighting Cybercrime in the Two Europes. The Added Value of the EU Framework Decision and the Council of Europe Convention', (2006) 77 *International Review of Penal Law* 503-24.

Gillespie, A. 'Sentences for Offences Involving Child Pornography', (2003) *Criminal Law Review* 81.

Gillespie, A, 'Tackling Child Grooming on the Internet: The UK Approach', (2005) 1 *Bar Review* 4.

Gringas, C. *The Laws of the Internet*, Butterworths 2002.

Hoekman, J. and C. Dirkzwager, 'Virtuele diefstal: hoe gegevens toch weer goederen werden', (2009) *Computerrecht* 158.

Kelleher, D and Murray, K, *Information Technology Law in Ireland*, Haywards Heath: Tottel 2007.

Koops, B.J. (ed.), *Strafrecht en ICT*, 2nd edition, The Hague: Sdu 2007.

Koops, B.J., 'Cybercrime Legislation in the Netherlands', country report for the 18th International Congress on Comparative Law, available at http://ssrn.com/abstract=1633958.

McIntyre, T.J., 'Computer Crime in Ireland: A critical assessment of the substantive law', (2005) 15 *Irish Criminal Law Journal* 1.

NCCRI, *Prohibition of Incitement to Hatred Act 1989: A Review, Submission by the National Consultative Committee on Racism and Interculturalism*, August 2001.

O'Malley, T., *Sentencing Law and Practice,* 2nd ed., Thomson Round Hall 2006.

Ormerod, D., *Smith and Hogan Criminal Law*, 12th ed, Oxford: Oxford University Press 2008.
Parker, D.B., *Computer Abuse*, Palo Alto 1973.