Legal aspects of online activities (Internet)

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Index

1. Introduction

This module looks briefly at the regulatory framework of online activities, in both civil and criminal law areas. This topic has been written on extensively, indeed it would need a whole book (rather, several) to cover all the relevant issues and the objective here is just to provide an overview of key topics: internet governance, online service provider liability and the regulation of electronic commerce and digital signatures. We will also look briefly at the fight against cybercrime.

First, as an introduction, we briefly comment on the initiatives for the protection of "digital rights" and on internet governance.

Online reading

- WSIS bibliography at http://www.itu.int/wsis/documents/bibliography.html provides an interesting list of readings on this topic.
- Other online reading includes:
  - European Commission: http://europa.eu/pol/infso/index_en.htm
  - The Internet Society: http://www.isoc.org/internet/law/
  - EFF: The Internet Law Treatise http://ilt.eff.org/index.php/Table_of_Contents
  - Stanford University: http://cyberlaw.stanford.edu/
  - Harvard University: http://cyber.law.harvard.edu/
  - BILETA: http://www.bileta.ac.uk/default.aspx

- Journals:
  - JILT: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/
  - Int. Jnl. of Law and Info. Technology: http://www.oxfordjournals.org/our_journals/inttec/editorial_board.html

1.1. Digital rights

The term "digital rights" describes the rights of persons in respect of the use of computers or electronic devices, or a communications network. In particular, the concept of digital rights relates to the protection of existing rights, such as the right to freedom of expression or privacy, in the online world, i.e. in the context of new digital technologies.

The rights in question that are considered relevant in an online context include fundamental human rights such as freedom of expression, privacy and freedom of association; and certain other important rights like the right to education or consumer rights.

These issues have mainly arisen as the extension of digital technologies into our lives has modified a previously existing balance between the individual and the state, and between individuals. The main thrust of the initiatives and regulation has been to protect existing rights in the new context (free speech),

and create or develop other rights in relation to technology within the context of protecting basic human rights and dignity in the digital "panopticon" (digital anonymity).

To a certain extent, the extension of certain rights to the digital context is fairly evident. Take for example two areas: free speech and privacy.

- As the internet is basically a communication tool, the right to free expression or freedom of speech is obviously a major issue, and has given rise to a series of cases and declarations regarding journalist rights, individual's rights to self-expression (through web 2.0 technologies such as blogs, twitter, etc.), the defence of criticism and parody, and how to deal with online defamation.

- The massive use of information (and the opportunity to massively use and connect information) combined with certain monitoring or privacy invasive activities – from the simple webpage cookie to data scraping and harvesting from the web to real-time monitoring of activities (Carnivore, key logging, etc.), has impinged on individuals' rights to privacy. This has in turn led to , giving rise to greater use of encryption (and thus the government's desire to regulate encryption technologies and private keys).

Other issues are not so evident:

- The determination of where an activity takes place (e.g. publication of defamatory work), so as to decide where to take action to protect or defend one's rights.

- The right to anonymity (e.g. using TOR networks or other identity hiding systems) and access by government to cryptographic keys (e.g. see the EFF site).

- Digital rights management systems that monitor or control a person's use of certain technologies (e.g. Sony Rootkit matter).

- Behaviour tracking on the web (e.g. Google's email screening; see the Working Party 29).

- Travel screening (the US control on air passenger information, see the EPIC and the Statewatch sites).

- Misuse of "cease and desist" letters (letters requiring certain information to be taken down or an activity to stop, alleging infringement of intellectual property or other rights). While these C+D letters are a valid means for defending a person's rights such as privacy or IP rights, they have often

been abused so as to censure legitimate activities such as criticism, reporting or linking (see the Chilling effects site).

This is not the space to cover these issues in great details, as this course focuses on technologies, however it is interesting to note that a series of initiatives have been undertaken in this area, which provide interesting further reading:

- The **World Summit on the Information Society** (WSIS). These conferences were set up in 2003 and 2005 under the United Nations. This summit was highly controversial (particularly regarding ICANN), aiming to provide a discussion forum and framework for the protection of rights in the digital environment, leading to significant negotiations between governments, businesses and civil society. This is an ongoing activity, and has currently lead to the WSIS Declaration of Principles, reaffirming human rights.

  WSIS Declaration of Principles

  The WSIS Declaration of Principles is a series of statements or principles aiming to establish "an information society accessible to all and based on shared knowledge". There is an associated "Action Plan" to bring more than 50% of the world's population online by 2015. The 67 principles affirm, among other things:

  - A commitment to build a "people-centred", inclusive and development-oriented Information Society.
  - The universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including freedom of opinion and expression.
  - The sovereign equality of states (i.e. no interference with internal matters... such as censorship!).
  - The recognition of diversity, special needs, the need to support the poor, and the need of inclusiveness, partnership and cooperation among governments and other stakeholders.
  - To meet these challenges by:
    - improving access to information and communication infrastructure and technologies;
    - providing access to information and knowledge;
    - building capacity and IT applications;
    - increasing confidence and security in the use of ICTs;
    - creating an enabling environment at all levels (legal, economic, social, standardisation, etc.);
    - recognising the role of the media;
    - addressing the ethical dimensions of the Information Society; and
    - encouraging international and regional cooperation.

  Work is ongoing, within the context of the "WSIS follow up" and the Tunis Agenda.

  One interesting aspect of WSIS from a technological point of view is the One Laptop Per Child initiative of Nicholas Negroponte, chairman and founder of the Massachusetts Institute of Technology Media Labs. This initiative was first presented at the WSIS and the objective was to present, at the 2005 Tunis meeting, a 100 USD laptop (running GNU/Linux, of course).

- The **Global Network Initiative** (GNI). This initiative was founded with a stated objective of "Protecting and advancing freedom of expression and privacy in Information and Communications Technologies". This oddly enough includes a series of a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics. These parties spent two years negotiating and creating a collaborative approach to protect and advance freedom of ex-

pression and privacy in the ICT sector. They have developed Principles and Guidelines and Governance charter for this purpose, to provide direction and guidance in relation to the use of ICTs.

The GNI Principles and Guidelines and Governance

The GNI principles are aimed at defending freedom of expression and privacy in ICTs, basically stating that ICT companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. The principles are based on the Universal Declaration of Human Rights and other international documents, and cover the following issues:

- Freedom of Expression. On top of the generally accepted principal of free speech and absence of government restrictions, the principles recognise that broad public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential.
  Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimise the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.
- Privacy: this is stated as a human right and guarantor of human dignity, important to maintaining personal security, protecting identity and promoting freedom of expression.
  Participating companies will employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users.

To implement these principles, the guidelines focus on:

- Responsible company decision making: integration of the principles into company management and culture.
- Multi-stakeholder collaboration: development of collaborative strategies involving business, industry associations, civil society organisations, investors and academics.
- Governance, Accountability and Transparency: implementing a governance structure and demanding accountability through transparency and public scrutiny.

- **European Digital Rights** (EDRi) is an international advocacy group founded in 2002 by members from several European countries to defend civil rights in the information society. This group monitors regulation regarding the internet, copyright and privacy in European and International institutions. They have covered data retention requirements, spam, telecommunications interception, copyright and fair use restrictions, the cyber-crime treaty, rating, filtering and blocking of internet content and notice-and-takedown procedures of websites.

- The **Electronic Frontier Foundation** (EFF) is an international non-profit digital rights advocacy based in the United States. Its stated mission is to defend free speech, privacy, innovation, and consumer rights online. EFF was one of the early players in defending digital rights, helping educational activities policy-makers (e.g. with regard to free and open telecommunications networks), raising public awareness about civil liberties issues arising from the rapid advancement in the area of new computer-based communications media; and, interesting from a legal perspective, supporting litigation to protect these rights. Among other issues, they have been active with regard to:

- P2P Technologies (MGM v. Grokster, INDUCE Act).

- Online journalism and defending the confidentiality of sources (Apple v. Does).
- Privacy protecting technologies (Bernstein v. U.S. Dept. of Justice).
- Online censorship (ACLU v. Reno / Communications Decency Act).

MGM v. Grokster

The content industry has been fighting against online peer-to-peer P2P file-sharing systems since Napster, in 1998. Their arguments are that these systems infringe the IP rights of the content holders, inducing and actually committing breaches of copyright. However, since the Sony v. Betamax case of 1984, the US courts have held that a company is not liable for creating a technology that some customers may use for copyright infringing purposes, so long as the technology is capable of substantial non-infringing uses. P2P file sharing systems themselves, while permitting users to share copyright protected works, are also used to distribute works under free content licences and works in the public domain. Napster was shut down (in the end, voluntarily) because the centralised system did in fact contain the works that were being shared, and thus the system itself was infringing IP rights. In the Grokster case, "Hollywood" sued Grokster, a distributor of the file-sharing software. In this case, Grokster itself never actually reproduced the shared works in its systems – just provided a mechanism for sharing the links. After lengthy legal battles, the courts did not overturn the Betamax doctrine, however found Grokster guilty of "secondarily liability" for IP infringement (i.e. not directly committing the act, but "inducing" it), stating that it actively promoted illegal file sharing, did not implement any filters on content passing through its systems, and built a business model based on the use of third party protected works.

Apple v. Does

In 2004, Apple took legal action against unnamed individuals who allegedly leaked information about new Apple products to several online news sites, in particular concerning a FireWire audio interface. Apple also filed a separate trade secret suit against a site called Think Secret in 2005. Apple sought the identities of the persons who had leaked the information to the journalists of these sites. EFF successfully defended the journalists and sites in question against revealing their sources, on the basis of the confidentiality of media sources.

Bernstein v. US Dept. Justice

In 1995, Daniel Bernstein, a Berkeley university researcher, planned to distribute an encryption program he had written (called Snuffle) that could help prevent third parties from intercepting online communications, discovering passwords and, for example, stealing credit card numbers. US laws (export control and traffic in arms regulation) restricted the publication of his program, as encryption technology falls within weapons control laws (Waasemar treaty), treated as a potential threat to national security. The US federal courts affirmed, for the first time, that software code deserves First Amendment (free speech) protection and thus Bernstein could publish the code and scientific papers about the algorithm.

ACLU v. Reno

In 1996, the US promulgated the Communications Decency Act, a law in favour of Safe Internet and criminalising the publication of certain content online (that the government could not prohibit offline). EFF and a group of interested parties (ACLU being one of them) questioned the constitutionality of the law and the Supreme Court eventually declared it unconstitutional on the basis of the protection of free speech. US Congress then passed the Children Online Protection Act (criminalising "commercial" distribution of material deemed "harmful to minors") and the courts have granted orders against its enforcement, basically for being too wide in scope.

- The **Open Rights Group** (ORG) is a UK-based organisation campaigning on digital rights issues and online freedom, and acts as a media clearinghouse service putting journalists in touch with experts, "*fostering a community of grassroots activists*". It campaigns against digital rights management (DRM), the extension of the term of copyright protection afforded to sound recordings, e-voting, as well as numerous other issues.

Other interesting organisations to follow include:

- **Statewatch** "monitoring the state and civil liberties in Europe".

- **European Civil Liberties Network** (ECLN) "seeking to create a European society based on freedom and equality, of fundamental civil liberties and personal and political freedoms, of free movement and freedom of information, and equal rights for minorities".

- **Electronic Privacy Information Center** (EPIC) "Focusing public attention on emerging privacy and civil liberties issues".

- **Foundation for a free information infrastructure** (FFII) "information about free and competitive software markets, genuine open standards and patent systems with lesser barriers to competition".

1.2. Internet governance

One topic that gave rise to significant concerns at the origins of the internet is the technology governance model (i.e. who regulates the communications network). While it is still an issue, it has gone off the agenda more recently, as other "hot topics" such as "content piracy" or "digital terrorism" have arisen.

Originally, the internet was a private (academic) and US-centred network, and governance was established on a closed model, carried out by engineers and scientists. The private sector provided a significant amount of the investment and infrastructure (the international backbone infrastructure, the national cable networks, and provides services that facilitate and manage traffic).

As regards communications standards and the technological operation of the internet, the IETF (Internet Engineering Task Force), a private body, developed certain technical rules for the functioning of the internet (protocol definition, etc.). They were reinforced by the W3C (world wide web consortium) defining standards and protocols for that part of the internet that is the world wide web.

However, overall, a key element of the network has been the resources for network names and addresses: domain names, IP addresses. Originally, the IANA (Internet Assigned Numbers Authority) was responsible for assigning internet names and addresses. However, the American government decided, in the late 1990s, to contract some of the services provided by IANA from ICANN (the Internet Corporation for Assigned Numbers and Names).

ICANN is a US non-profit public-benefit corporation and is responsible for coordinating the management of the Domain Name System (DNS), the allocation of internet protocol address spaces, the coordination of new internet

coordination parameters and the management of the internet's root name server system. While ICANN is a quasi private organisation, it is assisted and monitored by a Governmental Advisory Committee (GAC) which is open to all governments and a number of international organisations with a direct interest in ICANN policy, including ITU, WIPO, OECD, etc.

- **Domain names**: Domain names are names by which internet hosts may be easily identified, as opposed to the numerical IP addressing system used for network communication. ICANN set out two types of registry:
  - a number of generic top-level domains (gTLDs), such as ".com", ".net", and ".org" which are used worldwide (expanded to .biz, .info, etc.);
  - about 240 national or territorial registries maintain similar systems of names under a country code (ccTLD registries), such as ".uk", ".fr".

  National registrars were set up for the ccTLDs (Nominet, ES-NIC, etc.) and ICANN accredited a number of private registrars (like Verisign) for registering domain names.
- **UDRP** (Uniform Dispute Resolution Policy) is a process established for the resolution of issues regarding the registration and use of domain names, supervised at an international level by WIPO, and at national level by the corresponding registrars. We have commented on this issue in the module on trademark use on the internet.

While ICANN argues it has succeeded in maintaining the stability of the Domain Name System for ten years now, and encouraged a participative decision-making process, there have been a series of criticisms concerning its private nature, its lack of representativeness and even its monopolistic tendencies.

- The legal structure and incorporation of ICANN under Californian law poses problems, including conflicts of applicable law and jurisdictions.
- Legitimate concerns remain as to whether a governmental committee advising a private corporation is an appropriate and effective mechanism to enable governments to exercise their public policy responsibilities.
- On top of this, the self-regulatory approach as practised by ICANN means that incumbent operators play a potentially inappropriate role (e.g. from the standpoint of competition policy) in setting entry conditions for new competitors.

For further information on the topic, see an early article[1] and contrast with information at Icann Watch, GIPI and IGF.

(1)For example, at the Duke Law & Technology Review.

2. Online activities

We consider that it is important to have minimum knowledge of the rights and obligations regarding online activities, particularly in respect of internet related services (access, hosting, linking, etc.) and web platforms, both those that merely broadcast information ("passive" sites) as well as those of electronic commerce (dynamic sites), and the most recent social networks (Facebook, YouTube, Flickr, Twitter, etc.).

There has been a significant amount of legislation to adapt the legal frameworks of the "analogue world" to the digital world, the "Information Society". This has mainly occurred at regional (i.e. European) level, to harmonise laws between member states of the EU so as to remove barriers against electronic trading: both providing information society services, and online contracting.

- Applicable regulation in this area at EU level includes:
  - Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market. (Ecommerce Directive).
  - Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Copyright in the Information Society Directive).
  - Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts ("Distance Selling Directive").
  - Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Privacy Directive).
  - Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (IPR Enforcement Directive).

We have presented and commented on the last two Directives in the module on Intellectual Property Rights.

2.1. Information society services

The services supplied by the "*Providers of services of the information society*" are basically regulated on a European Level by the Electronic Commerce Directive, transposed nationally through various laws such as the Spanish "Ley de

los Servicios de la Sociedad de la Información y el Comercio Electrónico" or the English Electronic Commerce (EC Directive) Regulations 2002, Consumer Protection (Distance Selling) Regulations 2000.

In this section we will consider the administrative and legal framework for the provision of services (the scope of application of the regulations, administrative requirements and the legal regime applicable to international transactions) as well as the obligations that are binding for providers. In the following section, we will comment on electronic contracting and the regulation of commercial activities over the internet.

Online privacy issues are covered in the module on privacy.

The definition of information society services already exists in Community law in Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society; this definition covers "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".

Thus basically the Ecommerce Directive applies to all activities carried out by electronic means and having a commercial nature or pursuing a financial objective (to obtain financial income directly or indirectly). In other words, it applies to web pages that carry out electronic commerce activities as well as to those that supply information or offer services free for users, when they represent an economic activity for their owner.

The Directive and national laws cover both services between enterprises (B2B) and services between enterprises and consumers (B2C), as well as services provided free to the recipient (depending on the country, these may need to be financed, for example, by advertising income or sponsoring).

Information society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering online information or commercial communications, or those providing tools allowing for search, access and retrieval of data.

> It covers the all sectors and activities, including in particular: newspapers, databases, financial services, professional services (solicitors, doctors, accountants, estate agents), entertainment services (video on demand, for example), direct marketing and advertising and Internet access services.

2.2. Country of origin rule and applicable law

In an international environment such as the internet, it is important to determine the act that applies to the provision of a service. Otherwise, providers of services over the internet could be exposed to the control and applicable act of all the countries of the world. In order to avoid this problem, on a European level it has been ruled that, in most cases, the place where the service provider is established will determine the act and competent authorities that regulate them (the "country of origin" principle).

Thus under Article 3 of the Directive, providers of information society services are subject to the legislation of the Member State in which they are established. The Directive defines a provider's place of establishment as the place in which a service provider effectively pursues an economic activity using a fixed establishment for an indefinite period. Thus service providers established in France only need be concerned by French regulation, service providers established in Spain comply with Spanish laws, and so on (subject to what we mention below as to applicable law and jurisdiction, especially as regards consumers).

It is important to note that the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider. So a UK based service provider with equipment in France would not a priori be subject French regulation of its activities (except as regards consumer sales directed at France, see below).

2.2.1. Applicable law and jurisdiction

Another area of doubt is which law applies to online relations and which courts should solve differences (in the event of international issues). This has always been a difficult issue, an area of law called Private International Law or Conflict of Laws.

With regards to electronic contracting, in general the law and competent courts agreed in the contract will apply. Failing that, the standard rules of Private International Law will apply. With contracts between consumers and professionals – the applicable law is that of the country of residence of the consumer, provided that this is also the country where the professional carries out his/her activities or to which his/her activities are directed. The parties may also, based on freedom of choice, apply another law, as long as it provides the same level of protection to the consumer as that of his/her country of residence (This is why, for example, consumer product distribution platforms are often customised for each target country – for example www.pixmania.com).

As regards non-contractual obligations and liabilities (torts, IPR issues, etc.), the "Rome II" convention (since 2009, Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations) provides that the applicable law is:

- The law of the country where the damage occurs.
- The law of the country where both parties were habitually resident when the damage occurred.
- The law of the country with which the case is manifestly more closely connected than the other countries (using the "points of contact" doctrine").

As regards the courts that would hear any conflict ("jurisdiction"), this is also covered at European level and case law. Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (as amended) provides that:

- The basic principle is that jurisdiction is to be exercised by the Member State in which the defendant is domiciled, regardless of his/her nationality. This will always be the case for consumer defendants.
- Apart from the basic principle on jurisdiction, in certain circumstances a defendant may be sued in the courts of another Member State, including: (IPR issues, other).
  - Contracts: where the parties have agreed or where the obligation is performed.
  - Family maintenance: where the creditor (the person paying maintenance) is domiciled.
  - Torts (wrongful acts): where the harmful act occurred (including IP infringement).
  - Consumers: always in their own domicile (see next).
  - Insurance: where the insurer is domiciled.

- In order for the consumer to enjoy this protection in his/her home domicile in other cases, the consumer contract must have been concluded with a person either who pursues has commercial or professional activities in in the Member State in which the consumer's Member State (e.g. a local or national business), or is domiciled this company/professional "or directs" such these activities to that Member State (e.g. a business is domiciled in the UK, but has an online platform for selling products across the rest of Europe, including e.g international delivery, and the website is in several European languages; in this case, the consumer can argue that the platform is directing its activities at the consumer in another country).
- A consumer may either bring proceedings either in the courts of the Member State in which the defendant is domiciled or in the courts for the place where the consumer (as plaintiff) is domiciled.

2.3. Service Provider obligations

In order to provide services over the internet, companies do not need to request authorisation or sign any registry. However, with a view to improving the transparency of "remote" commerce, service providers are obliged to publish certain data about themselves and their products.

- **General information obligations**. Service providers must indicate on their web page:
  - Their company name and contact details (address, email address and any other detail allowing direct and effective communication, for example a telephone or fax number).
  - If the company is inscribed in the Company Register or any other public register, stating also the corresponding inscription number.
  - The company's tax identification number (for VAT purposes).
  - Information regarding product prices, whether or not they include applicable taxes, delivery costs, and any other data that ought to be included under applicable norms of the autonomous communities.
  - Details regarding any administrative authorisation where necessary, as well as the relevant supervisory body.
  - Details of the professional body for regulated professions (Lawyers, attorneys, doctors, etc.), and the affiliation number, academic qualification and State of the European Union that issued it with the corresponding approval where applicable.
  - Codes of Conduct adhered to, where applicable, and the means of consulting them electronically.

- **Obligations regarding cookies and security**. The use of *cookies* is not prohibited, since they are sometimes necessary in order to facilitate communications or to customise websites, however, as a modification to the original Directive, service providers must provide clear and complete information on the use and purpose of *cookies*, offering the possibility of rejecting the processing of data through a simple and free procedure (basically, by deactivating them in the browser).
  At the same time, *internet access suppliers* are obliged to inform their users (for example, on their main web page or site), about:
  - the technical measures that ensure protection against security threats over the internet (computer viruses, spyware, spam),
  - tools for filtering unwanted content,
  - security measures applied in the provision of their services (together with email service providers),
  - potential liabilities that could be incurred through use of the internet for illicit purposes.

- **Additional obligations to collaborate and liability of intermediate service providers.** There is also an additional provision, articles 15 and 19, requiring member states to ensure the service provider supplies (and

thus collaborates with) national authorities (administrative and police) with "requisite information", specifically regarding alleged illegal activities, when so required , e.g. in order to interrupt the provision of a service or to identify an online user.

However, the law releases from liability certain internet "intermediaries"– access, data transmission, hosting and search engine services – with regards to the contents that they host, transmit, provide access to or classify in a link directory (see below). They are not obliged to supervise said content, for example. But they can be liable if they take an active part in its preparation or if, knowing that particular material is illegal, they do not act speedily to remove it or to prevent access to it.

3. Liability of information society service providers

Not all of the information transmitted through the internet is in compliance with national legal systems. The dissemination of some information is unlawful, e.g. images related to child pornography or works protected by intellectual property rights (for instance, the online publication of music or video works without authorisation). The diffusion of such content interferes with public or private interests.

The legal responsibility is borne by the authors of the online publications. Nonetheless, the question of intermediaries on the communication networks arises. Those intermediary players serve to transmit and host information and to provide access to a communication network (ISPs – Internet Service Providers).

The intermediaries do not have real control over all the information transmitted through their equipment. It would be expensive and technically difficult. Furthermore, considering intermediaries liable could be prejudicial to the development of the internet.

For that reason, the Ecommerce Directive provides a balanced solution for the interests at stake and aims to end the growing differences between Member States' legislation and case law that were emerging on the liability of internet intermediaries.

The directive does not just apply to copyright infringement but is established in a horizontal manner, so that it applies to all kinds of illegal materials (including copyright, unlawful commercial practises, breach of privacy, criminal liability, etc.).

However, to benefit from the protections, the service provider must be an "intermediary" and, therefore, the information must be provided by the third party recipients of services and must be transmitted or stored at their request.

The European directive covers three categories of online intermediary activities, and different conditions must be fulfilled for each one.

3.1. Activities covered and conditions for liability limitation

This directive creates a system that prevents online intermediaries from being held liable for specific activities under certain conditions.

For the activities or intermediaries not covered by the directive, or for intermediaries that do not fulfil the liability limitations conditions, the Directive refers to the applicable national law of liability of Member States.

Primarily, the Directive prohibits member states from obliging ISPs to monitor the content of the data they process. However, to benefit from the exemptions, they must satisfy the conditions, on an ongoing basis:

- **Mere conduit:** A mere conduit is defined as "*a service provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*." It refers, for instance, to the functions of an internet access provider or network operators. An intermediary engaging in mere conduct activity will not be liable for the damages caused by the information transmitted as long as it does not:
  - Initiate the transmission.
  - Select the receiver of the transmission.
  - Select or modify the information contained in the transmission.

The provider cannot play an active role in the transmission of information. Its role has to be limited to the technical process of operating and giving access to a communication network. The condition of not having modified the information does not extend to the technical manipulations enabling the transmission of information since these do not alter the integrity of the information contained in the transmission.

Thus, insofar as the provider has a passive and neutral role, it may not be held liable for the information transmitted through its equipment, either at a civil or at a criminal level.

1) Caching: Caching consists of "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request". Any intermediary provider that carries out a caching activity will not be held liable as long as it meets the following conditions:

- It does not modify the information.
- It complies with conditions for accessing the information.
- It complies with rules for updating the information, specified in a manner widely recognised and used by industry.
- It does not interfere with the lawful use of technology widely recognised and used by industry to obtain data on the use of the information.
- It acts expeditiously to remove or disable access to the information it has stored upon obtaining knowledge of the fact that:
  - The information at the initial source of the transmission has been removed from the network.
  - Access to it has been disabled.

– A court or an administrative authority has ordered such removal or disablement.

In other words, the intermediary provider must stay neutral concerning the content of the information.

2) Hosting activity: Hosting is defined as an information society service that consists of the "storage of information provided by a recipient of the service and at his request."

For instance, it includes the activities of the internet access providers who provide space on a server in order to store their clients' websites and therefore make them accessible on the internet.

To enjoy the liability limitation, the provider of hosting activities must:

- not have actual knowledge of illegal activity or information and,
- upon obtaining such knowledge or awareness, act expeditiously to remove or to disable access to the information.

Therefore, the intermediary providing hosting will be held liable if it is proven that he had knowledge of the existence of unlawful information (for instance by third party notification denouncing the existence of such information) and did not remove it or disable access to it.

There are differences as regards implementation of these provisions, with some national laws requiring effective knowledge of an illegal act through court order (so that the ISP does not have to take a decision as to whether some material is infringing or not) or through being served private notice (e.g. a take-down notice).

3.2. Other activities

Interestingly, certain national legislation has extended the ecommerce directive protections to other intermediary activities, namely linking and search engines.

- **Links**: Hyperlinks are at the base and origin of internet technology. They constitute technical mechanisms that, like pointers, permit a logical link to be made between different hypertext contents, allowing for highly dynamic browsing and obtaining of contents. While it is generally thought that no liability arises in respect of links created to infringing or illegal materials, unless "sponsoring" these materials, Spain for example has explicitly excluded liability for links where the linker does not know of the

nature of the data to which he/she is linking and removes the link when he/she does have such knowledge.

- **Search engines**. Search engines like Google or Yahoo are also essential features of the net, enabling information to be found among literally millions of pages. Again, it is thought that search engines should not be liable for the content of the pages they link to as a result of a search, and specific exemption has also been given in the same conditions as for linking. This is not the case, however, for search engines "caches", when they fall outside the caching exemption commented above, as often these search engines themselves store old or removed (illegal) information and thus provide access to it.

Linking and other forms of internet features such as metatags in general have caused a series of case law and decision, with the courts approaching the matter in different ways. In particular, they have considered:

- **Linking** is generally held (Shetland Times) to be legal, provided the actual text o f the link itself is not a breach of tirad third party Rights (e.g. copyrighted work, such as – arguably – a newspaper title – see Shetland Times case, where a newspaper used the headlines of a competing newspaper to link to that paper, bypassing the front page.

- **Deep linking**: linking to a page that is not the "home" page of the linked site. Again this has been deemed to be licit, as it is understood that the whoel point of havinge "pages" is to be able to link to any of them, and the linked website owner has technical means for preventing linkers going direct to a sub-page.

- **Framing**: using a separate segment of the browser to display another company's linked webpage, not explicitly showing its URL – i.e. creating a frame round the linked site. This is generally understood to be a breach of the linked site owner's rights, if not unfair competition (where the linked content cannot be distinguished from the linker's own content, thus causing confusion). This is even more so when the framed content includes trademarks and other protected works.

- **Inlining**: creating webpages from third party content (stored on another site). Again, if the third party content is protected by copyright, it is generally considered to be illegal to "inline", at least when it is done without attribution. This is more controversial, for example, when search engines inline thumbnails or abbreviated parts of third party content. Again this is a technical issue, as the thumbnails or extracts themselves may not be inlined, but reproduced by the linking site.

- **Metatags** are a means of using certain data to mark up or inform on the content of a site. Certain sites will use trademarks and other protected signs to attract search engine attention (thus rising in the results ranking) – a practice which is generally considered illegal unless authorised by the rights holder or benefitting from other exemptions (fair use).

  For more reading: see Bechtold's page (updated to 2004 only) and more information at the Wikipedia site. Also commented at Bitlaw Legal Resource.

Bibliography

See for example http://searchenginewatch.com/2156551, comment at http://cyber.law.harvard.edu/property00/metatags/main.html and http://ilt.eff.org/index.php/Trademark:_Links,_Frames,_Search_Engines_And_Meta-Tags.

3.3. ISPs and IPR enforcement

While ISPs may benefit from exemptions with regard to the data they process on behalf of others, we have seen in the module in IPR that Directive 2004/48/EC on the enforcement of intellectual property rights (IPR Enforcement Directive), requires certain involved parties to provide information on the possessors of infringing products, the recipients of infringing services and those that have provided services to the infringer.

Thus in the field of e-commerce, the question may arise whether the intermediary service provider has the obligation to provide information on the recipients of its services (the infringers/the content providers carrying out illegal activities), or is exempted from such obligation by referring to the regulations on limitation of liability and exemption from monitoring obligation set out in Ecommerce Directive.

Under Article 8 of the Enforcement Directive, Member States must ensure that in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of a claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:

- Was found in possession of the infringing goods on a commercial scale.
- Was found to be using the infringing services on a commercial scale.
- Was found to be providing services used in infringing activities on a commercial scale.
- Was indicated by the person referred to in points (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.

The Enforcement Directive determines the scope of the information to be provided and regulations to be taken into account when enforcing the right to information – in particular, regulation as to the processing of personal data. So ISPs find themselves at the heart of a conflict between three laws (IPR, Privacy, Ecommerce).

ISPs are usually the target of IPR enforcement activities as they hold the data to identify users (IP address / domain name) and often host the allegedly illegal materials. Therefore, the question may arise whether the ISP has the obligation to provide information on the recipient of its service, the content provider committing infringement, or may be exempted from such obligation by referring to the regulations on liability limitation (Sections 7-13 of Ecommerce Directive) or the exemption from monitoring obligations (Section 7 (5) of Ecommerce Directive).

It is understood that the Enforcement Directive generally does not affect the principles of the Ecommerce Directive and does not at all affect the limitation of liability existing in favour of the intermediary service providers and set out in Articles 12-15. The introduction of the right to information is only compulsory in cases of illegal activities or services carried out on a commercial scale (for direct or indirect economic or commercial advantage; this would normally exclude acts carried out by end consumers acting in good faith). So that is already one area of comfort for ISPs.

However, it is also understood, on the basis of the recitals to the Ecommerce Directive, that limitations of the liability of ISPs do not affect the "possibility of injunctions of different kinds; such injunctions can, in particular, consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it." This is reinforced by information and collaboration obligations set out in national implementations of the Ecommerce Directive.

Thus it is not a question of what ISPs have to do, but when and how: do they need a court order (so they are not considered to censure their user's content and breach privacy laws) or is it sufficient for a notice? This is an issue that is still unresolved, and will depend on how national laws are implemented and interpreted by courts.

So far, court cases vary (see L'Oréal –v– eBay in England, which has been referred to the ECJ), but on the whole intermediaries have escaped significant liability, e.g. in the recent Google Adwords case (Court of Justice of the EU, 23 March 2010, Cases C-236/08 to C-238/08). But IPR holders will not stop there.

4. Ecommerce – Online Contracting

Supplementary content

It will be important to include these processes in the design (and budget!) of any interactive portal and the "back-office" systems that support it.

Beyond the "information society service provider" information obligations and ISP exemptions, the ecommerce regulations deal with electronic contracts and online contracting, and oblige certain processes to be implemented for the correct sale of products over the internet (presented in this section).

4.1. Valid electronic contracts

National laws pursuant to the Ecommerce Directive must guarantee the validity and effectiveness of contracts celebrated electronically, even if there is no copy in paper format. In other words, a contract's electronic format is equivalent to that written on paper and the effectiveness of electronic documents as proof in court is reinforced (also admissible as evidence in court proceedings, as we discuss below in relation to the electronic signature whereby electronic signatures are equivalent if not better than manuscript signatures).

4.2. Information and processes

In order to guarantee the legality of the contracting process, on the basis of the Ecommerce Directive and the Distance Sales Directive, service providers must establish certain minimum processes:

- Before initiating the contracting procedure, the following information must be made available to the user, in a simple, free, clear, understandable and unequivocal manner:
  - The steps or processes to be followed in order to enter into the contract.
  - Whether the electronic document of the contract will be filed and whether it will be accessible.
  - The technical means made available in order to identify and correct errors in data input, before data is confirmed.
  - The language or languages in which the contract may be held.
  - The general conditions governing the contract, where applicable.

- Once the contract has been entered into, the provider must confirm receipt of the contract's acceptance (by means of an acknowledgement of receipt by email or similar, or other equivalent means of communication to that used in the contracting process – sales confirmation screens, for example with an order or reference number).

These electronic contracting processes can be verified on most e-commerce sites, for example, for the purchase of train or plane tickets, or downloads of commercial software (antivirus packages, etc.). They allow buyers to check the general conditions of the sale,

and oblige them to accept these (ticking an "accept" check box) before confirming the purchase.

4.3. Obligations associated with remote selling to consumers

For the protection of consumers, national contract law may still affect B2C (Business to Consumer) transactions, which are deliberately not subject to country of origin principle: usually the national law of the consumer's country applies.

Luckily, consumer protection law is partly harmonised in the EU, including

- The Distance Selling Directive provides for the consumer's right to withdraw contracts and for different performance and credit card provisions.
- The Directive on unfair Terms in Consumer Contracts imposes the exclusion and limitation of liability.
- The Consumer sales and guarantees Directive establishes minimum levels of guarantees.

There is on the table a proposal to review and consolidate EU consumer protection laws.

In particular, the framework provide for:

- The provision of comprehensive information before the purchase.
- Confirmation of that information in a durable medium (such as written confirmation).
- Consumer's right to cancel the contract within a minimum of 7 working days without giving any reason and without penalty, except the cost of returning the goods (right of withdrawal).
- Where the consumer has cancelled the contract, the right to a refund within 30 days of cancellation.
- Delivery of the goods or performance of the service within 30 days of the day after the consumer placed his order.
- Protection from unsolicited selling.
- Protection from fraudulent use of payment cards.
- Non-validity of any waiver of the rights and obligations provided for under the directive, whether instigated by the consumer or the supplier.

Some types of contracts are excluded from these obligations, including contracts for financial services and contracts concluded through an auction (NB: contracts for financial services are covered by the Distance Marketing of Financial Services Directive 2002/65/EC.).

4.4. Commercial communications and publicity

Finally in the area of ecommerce, laws have set out provisions regulating "commercial communications" – "spam", when unsolicited (Art 7 Ecommerce Directive, as updated by Privacy Directives). These require the addressee's prior consent, both for email as well as for mobile messages. Nevertheless, the sending of commercial communications to those users with whom there is a previous contractual relationship is allowed, in which case the provider may send publicity regarding similar products or services to those contracted by the client.

For the protection of users, the provider must offer the addressee the possibility of opposing the processing of his data for promotional purposes, both at the time of collecting the data as well as in each commercial communication addressed to him. This option tends to be hidden in the general conditions of sale or subscription, which the user accepts when registering or confirming a purchase over the internet. The service provider must establish simple and free procedures for this purpose, as commented below in the section on data protection.

For the purpose of maintaining transparency and protecting the consumer, electronic publicity (emails, web pages, "YouTube" videos) must be presented as such, so that they cannot be confused with any other type of content, and clearly identify their nature to the advertiser.

Promotional offers (in other words, those that include gifts or prizes, or discounts, and competitions, or promotional games, etc.) must be clearly identified as such and the conditions of access and participation must be easily accessible and expressed in clear and unequivocal terms.

5. Electronic signatures

One of the areas of work of legislators over the last 10 or more years has been the use of electronic signatures and documents, to replace written signatures and paper copies of contracts, administrative forms and other commercial and administrative "documents". The basic framework at European level is Directive 1999/93/CE of the European Parliament, of 13 December 1999 establishing community framework for electronic signatures.

At this level, the regulations state that whenever certain minimum requirements are met in relation to the certificates, **then equivalent legal effectiveness is given to the electronic and handwritten signatures**. The Directive goes on to establish the criteria for legal acknowledgement of the digital signature, focusing on the services of certification.

These include:

- Common obligations for certification service providers in order to secure transborder recognition of signatures and certificates throughout the European Community.
- Common rules on liability to help build confidence among users, who rely on the certificates, and among service providers.
- Cooperative mechanisms to facilitate transborder recognition of signatures and certificates with third countries.

5.1. Electronic signatures

The Directive defines various forms of electronic signatures:

- **The electronic signature**, being data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. This could be an email signature.
- **The advanced electronic signature**, which meets the following requirements:
  - It is uniquely linked to the signatory.
  - It is capable of identifying the signatory.
  - It is created using means that the signatory can maintain under their sole control.
  - It is linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.

- **The qualified certificate, which must in particular include:**
  - An indication that it is issued as a qualified certificate.
  - The identification of the certification service provider.

- The name of the signatory.
- Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended.
- Signature-verification data corresponding to signature-creation data under the control of the signatory.
- An indication of the beginning and end of the period of validity of the certificate.
- The identity code of the certificate.
- The advanced electronic signature of the issuing certification service provider.

The certificate must also be issued by a certification service provider, which meets specific requirements laid down in the Directive, establishing minimum requirements for recognition across Europe.

To guarantee pan-European market access and recognition of signatures, the Directive prohibits Member States from making the provision of certification services subject to prior authorisation of any kind (they may introduce or maintain voluntary accreditation schemes aimed at enhancing levels of certification-service provision), nor may they limit the number of accredited certification service providers for reasons which fall within the scope of the Directive; nor may they restrict the provision of certification services originating in another Member State in the areas covered by the Directive.

5.2. Legal effects of electronic signatures

The main provision of the Directive states that an advanced electronic signature based on a qualified certificate created by a secure-signature-creation device satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data (for convenience this type of signature is usually called a "qualified signature". It is also admissible as evidence in legal proceedings.

In addition, an electronic signature may not legally be refused simply because:

- It is in electronic form.
- It is not based on a qualified certificate.
- It is not based upon a qualified certificate issued by an accredited certification service provider.
- It is not created by a secure signature-creation device.

Spain had legislated on the electronic signature in 1999, but came back to it in 2003 to adapt the regulation and transpose the directive mentioned above in Act 59/2003, of 19 December, on the electronic signature. The latter regulates the legal effectiveness of the electronic signature and the provision of certification services.

More recently, Act 56/2007, of 28 December, on Measures to Promote the Information Society modifies some precepts of the Act 59/2003, incorporating a new obligation for the Public Administration and certain companies, which entails the use of recognised electronic signature certificates in relations with citizens and clients, respectively.

6. Cybercrime

The growth of the Information Society has been accompanied by new series of crimes and misdemeanours, either directly against information society technologies (e.g. denial of service attacks, etc.) or using these technologies to commit traditional crimes such as fraud. The ITU believes that attacks against information infrastructure and internet services now have the potential to harm society in new and critical ways, due to the fundamental importance that these services and networks acquire in today's society and economy. Online fraud, the dissemination of child pornography and hacking attacks are just some examples of computer-related crimes that are committed on a large scale.

6.1. Introduction

The legal, technical and institutional challenges posed by the issue of *cybercrime* and its counterpart, "cybersecurity", are global and far-reaching, and it is thought and has been argued that it can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

Certain steps have been taken, both in the policy and the legal arenas. As regards policy, for example, the World Summit on the Information Society (WSIS) recognised the risks posed by inadequate cybersecurity and included it on its agenda in the 2003 and 2005 conferences. This led to the ITU setting up the Global Cybersecurity Agenda (GCA) in May 2007, a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity. Among the GCA work areas, the work on "*Legal measures*" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.

Due to the "novelty" of cybercrime (compared with crimes such as murder or theft), dealing with it requires first of all the necessary substantive criminal law provisions to criminalise acts such as computer fraud, illegal access, data interference, digital copyright violations and child pornography. Note that the fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network (e.g. creation or distribution of child pornography in paper format), does not mean that they can be applied to acts committed over the internet as well, because of the strict interpretation of criminal law.

> The computerisation of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago. The effective prosecution of these acts

requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles.

Then, once the crimes are defined, by substantive criminal law provisions, law enforcement agencies need the necessary tools and instruments to investigate cybercrime, using the same tools that the perpetrators use.

On a wider scale, the concept of "safe internet" has been used to cover the attempts to make the internet safer (and protecting internet users) and has become integral to the development of new services as well as governmental policy. Initiatives in this area are both public (e.g. the European Commission work) and private (e.g. Safe Internet Alliance).

6.2. Definitions and typology of cybercrime

One of the first difficulties has been the definition of "Cybercrime". Considerable difficulties have arisen in defining the term, but a general consensus is building towards it being defined as "any activity in which computers or networks are a tool, a target or a place of criminal activity" or "computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks"*.

See Convention on Cybercrime – Council of Europe Convention on Cybercrime (CETS No. 185).

Once we have a definition, we can study what activities specifically fall within the concept and see the measures that have been taken against them.

To assist in understanding the scope and scale of cybercriminal activities, a useful starting point is the Council of Europe Convention on Cybercrime (2001), being an International Treaty signed and ratified by most European countries and with additional parties such as USA, Canada, Japan, and Mexico. This Convention distinguishes between four different types of offences, set out in the following table:

Category	Specific crimes
Offences against the confidentiality, integrity and availability of computer data and systems	Illegal Access (Hacking, Cracking)
	Data Espionage
	Illegal Interception
	Data Interference
	System Interference
Content-related offences	Erotic or Pornographic Material (excluding Child-Pornography)
	Child Pornography
	Racism, Hate Speech, Glorification of Violence

Category	Specific crimes
	Religious Offences
	Illegal Gambling and Online Games
	Libel and False Information
	Spam and Related Threats
	Other Forms of Illegal Content
IPR-related offences	Copyright-related Offences
	Trademark-related Offences
Computer-related offences (offences that need a computer system to be committed)	Fraud and Computer– related Fraud (e.g. auction fraud)
	Computer-related Forgery
	Identity Theft
	Misuse of Devices (Carry out DoS attacks, designing and distributing computer viruses, Decrypt encrypted communication, Illegally access computer systems)

Obviously, there is significant disagreement between countries or areas with different cultures regarding the illegality of certain activities: while there is general agreement that child pornography should be prevented in all forms and manners, adult pornography is generally acceptable in most western societies. But within these, for example, there are significant different views on gambling, racism and hate speech (witness France and Germany's prohibition of any defence or promotion of Nazism, whereas USA tolerates this under its Freedom of Speech principles).

In Europe, child pornography in particular has had additional legislation, among others:

- The European Union Council Framework Decision on combating the sexual exploitation of children and child pornography (2003).
- The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007).

On the other hand, gambling for example has widely differing regulation over and outside the internet and the effect of different regulations is evident in success of "off-shore" gambling countries (Malta, Bahamas, UK...).

6.3. Technical and legal challenges

A number of challenges to creating an efficient international framework and process for dealing with cybercrime have been identified, most of the posed by the very technologies that underlie the Information Society:

- **Reliance on ICTs**: the greater the reliance our society has on ICTs, the more vulnerable it is to widespread attacks and the greater the impact.

- **Number of Users**: the increasing number of ICT users makes it increasingly difficult to identify criminals ... and increasingly easy for them to identify targets.
- **Availability of Devices and Access**: cybercrime was not really a public issue until personal computers and access to global networks became widespread, and with new and more sophisticated devices (mobile phones, "pads", etc.) and the pervasiveness of computing (home, office, etc.).
- **Availability of Information**: the global networks have given rise to easy access on topics such as how to make a home-made bomb, how to write computer viruses, etc.
- **Missing Mechanisms of Control**: the internet has no global regulator other than for technical reasons (DNS), which makes it difficult for authorities to exercise their powers.
- **International Dimensions**: Police forces and judicial authorities have local, regional or national jurisdiction, and processes for pursuing criminals across digital borders have not adapted with the speed of the networks.
- **Independence of Location and Presence at the Crime Site**: crimes may be initiated in one place, cause damage in another and the criminal may be located in a third (e.g. online publication by a person in France on a UK web-server that is defamatory to a person in Spain).
- **Automation and speed of data exchange processes**: automation speeds up the spread of illegal content, damaging malware and other criminal activities. By the time the authorities intervene, often there is no longer any trace of the criminals.
- **Anonymous Communications**: while total anonymity is difficult to achieve, technologies are built to protect individuals' privacy... with the effect also of assisting hiding the identity of those engaging in criminal activities.
- **Encryption Technologies**: this is becoming a target of national crime fighting authorities, as one of the most important steps in any criminal investigation is identifying the person who committed or participated in a criminal activity.

From a legal point of view, there are further difficulties in dealing with cybercriminal activities:

- **Drafting criminal law**: the speed of technological development means that law-makers must continuously respond to internet developments and monitor the effectiveness of existing provisions. The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law.
- **New Offences**: often, crimes committed using ICTs are not new crimes, but illegal activities modified to be committed online. This can normally be dealt with is the drafting of existing criminal legislation is wide enough to cover the new technological means or circumstances. The situation is

different, if the acts performed are no longer addressed by existing laws, so it becomes necessary to adopt new laws criminalising computer-related fraud, in addition to the regular fraud.

- **Use of ICTs**. It is ever more important for law enforcement agencies and the judicial authorities to use ICTs within their functions for dealing with ICT related crime. New tools mean the need for more training and new investigative instruments (within the area of digital forensics).
- **Digital Evidence**: digital evidence – data stored or transmitted using ICTs that may show how an offence occurred – is now not just a "new source of evidence", but is becoming a principal source of evidence. Handling this digital evidence has unique difficulties (to preserve integrity and make it available in court) and requires specific procedures.

New developments such as cloud computing can have a significant effect on dealing with digital evidence. Enforcement agencies can no longer simply focus on the suspect's premises – today a lot of computing is done online with online tools and repositories for remote access. These may well be outside jurisdiction.

6.4. International dimension

One of the major challenges is that cybercrime often has an international dimension. Criminal law is usually national law, and other than war crimes there is little international legislation in this area. Cybercrime is the one area where in fact progress has been made to deal with international criminal activities, or simply local criminal activities that use international networks. In terms of illegal content, for example, internet users can access information from around the world, enabling them to access information available legally abroad, that could be illegal in their own country.

Within cybercrime investigations, a close cooperation between the countries involved is very important. This has been the focus of EU action, which cannot regulate crime but can provide a pan-EU system for police cooperation. However, a number of countries base their mutual legal assistance regime on the principle of "dual criminality" (international investigations are limited to those crimes that are criminalised in all participating countries). One of the key aims of international legal approaches is to prevent the creation of safe havens by providing and applying global standards.

At EU level, there have been several initiatives and legal documents:

- Eurojust.
- Communication on "Network and Information Security (2001). Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.
- Framework Decision on Attacks against Information Systems (NB this has been challenged and partially invalidated by the European Court of Justice for lack of legal basis).

- Data retention Directive: EU Directive on Privacy and Electronic Communication (see privacy module).

In 2008 the European Union started a discussion about a Draft Amendment of the Framework Decision on Combating Terrorism. The EU highlights that the existing legal framework criminalises aiding or abetting and inciting but does not criminalise the dissemination of terrorist expertise through the internet. With the amendment the European Union is aiming to take measures to close the gap and bring the legislation throughout the European Union closer to the Council of Europe Convention on the Prevention of Terrorism.

For a general overview, see the Justice, freedom and security area of the European Union and in particular the judicial cooperation in criminal matters.

Other international initiatives are:

- ITU Global Cybersecurity Agenda.

- Council of Europe:
  - *Convention on Cybercrime* that we have already mentioned and comment on below. In addition to the signatories, other countries such as Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have already drafted parts of their legislation in accordance with the Convention.

  - *First Additional Protocol to the Convention on Cybercrime*, covering racism and the distribution of xenophobic material (this was a controversial matter especially due to the conflicts with freedom of speech principles).

  - *Convention in on the protection of minors against sexual exploitation* (2007). Apart from the criminalisation of the sexual abuse of children the Convention contains a provision dealing with the exchange of child pornography and the solicitation of children for sexual purposes.

- OECD: OECD Guidelines for the Security of Information Systems and Networks., at

As a result of the difficulty of enforcing national criminal law in a context of international networks, national approaches tend to require additional measures (crimes) so as to be able to apply local law to these activities. One approach is to criminalise the provision or use of services (within jurisdiction) used in the committing a crime. This puts an additional burden on service providers, to police their own networks (see the debate on IPR enforcement and the HADOPI law in France, soon to be replicated to a certain extent in Spain and maybe the UK). This does not always work as most crimes are not strict liability but require an element of knowledge (*mens rea*) so that network service providers can avoid liability by arguing lack of knowledge. The EU

Ecommerce Directive bases ISP exemptions on this argument, and only engages their liability when they have effective knowledge of the activity or sufficient ancillary indications.

Hadopi Law – Loi favorisant la diffusion et la protection de la création sur Internet

In May 2009 France promulgated a law to control and regulate internet access as a means to encourage compliance with copyright laws. "HADOPI" is the government agency created by the law to monitor enforcement.

HADPOPI: *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* (High Authority of Diffusion of the Works and Protection of the Rights on Internet.

The general idea is "three strikes and out", meaning that after HADOPI has given a first warning to internet users if it suspects the user is carrying out illegal activities (i.e. subtext: file sharing), the ISP must monitor the internet connection. If the user does not stop, a second letter may be sent by HADOPI, the ISP or the rights holders. If the use still doesn't stop, the ISP is required to suspend the service for 2 months up to 1 year (and the user is blacklisted from getting services from other ISPs).

This raises serious questions regarding fundamental rights, including as to privacy (ISP monitoring the service), access to information (suspension of the internet connection), burden of proof and right to a judicial defence, etc.

Spain has a similar project underway (with a similar commission) and the UK, in April 2010, passed the controversial Digital Economy Act[2], including rights to block internet access, obligations on ISPs to notify users if the ISP itself is notified by IP rights holders that there "appears" to be an infringement.

[(2)]See it online at the OPSI (Office of Public Sector Information) site, comment at the Open Rights Group site and Wikipedia.

6.5. Substantive (cyber) criminal law

While this is not the place for a full treatise on cybercrimes, in this section we comment on some of the most important measures against cybercriminal activities, focussing on the Convention on Cybercrime (CoC).

- **Offences against the confidentiality, integrity and availability of computer data and systems:**
  - **Illegal Access (Hacking)**. The CoC criminalises "unauthorised access to a system" thus protecting the integrity of the computer systems (Article 2 – Illegal access).
  - **Illegal Interception**. The CoC includes a provision protecting the integrity of non-public transmissions by criminalising their unauthorised interception (Article 3 – Illegal interception).
  - **Data Interference**. The CoC includes protects protection of the integrity of data against unauthorised interference. It provides computer data and computer programmes with protections similar to those enjoyed by tangible objects against the intentional infliction of damage (Article 4 – Data interference).
  - **System Interference**: To protect access of operators and users to ICTs, the CoC includes a provision criminalising the intentional hindering of lawful use of computer systems (Article 5 – System interference)

i.e. any act interfering with the proper functioning of the computer system.

- **Content-related offences:**
  - **Child Pornography**. The CoC includes an Article addressing child pornography to improve and harmonise the protection of children against sexual exploitation (Article 9 – Offences related to child pornography). This is reinforced by Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

- **IPR related offences:**
  - **Copyright infringements** (e.g. allegedly P2P file sharing, etc.) is a major concern of the content industry, which has significant presence and pressure in legislative circles. The CoC therefore includes provisions covering these copyright offences that seeks to harmonise the various regulations in the national laws (Article 10 – Offences related to infringements of copyright and related Rights). Unlike other legal frameworks the convention does not explicitly name the acts to be criminalised, but refers to a number of international agreements that already deal with this issue (WIPO Treaties, etc.).

- **Computer-related offences:**
  - **Computer related Fraud**. The CoC aims to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property (Article 8 – Computer-related fraud): "a. any input, alteration, deletion or suppression of computer data; b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

6.6. Procedural Law

As noted above, while achieving consensus on the definition and scope of various cybercrimes is one area, the other side of the coin is the introduction of procedures to enable enforcement agencies to take effective action against cyber-delinquency (in addition to training and equipment): procedural instruments that enable them to take the measures that are necessary to identify the offender and collect the evidence required for the criminal proceedings.

The main issue here is the digital nature of the evidence that is processed (collected, stored and produced), and the new media/means for transmitting it: the global ITC networks. This has led to the development of a new investiga-

tory "science", Computer Forensics (including computer and network Investigations) being specific data-related investigation techniques, including collection and analysis of relevant data.

Specific measures to facilitate the detection of cybercrimes include;

- Data retention obligations (obligation to preserve certain data at all times, e.g. traffic data) (Art. 16 CoC).
- Data preservation obligations (orders to preserve certain data once notified, not just limited to traffic data) (Art. 17 CoC).
- Data production obligations (orders to produce and disclose retained or preserved data) (Art. 18 CoC).
- Search and seizure orders (Art. 19 CoC).
- Real Time Collection of Data (Art. 20 CoC).
- Data interception (Art. 21 CoC).

On the other hand, care must be given to protect basic human rights and freedoms, ensuring that traditional safeguards are maintained in the digital environment. Criticism has been focused on the Convention on Cybercrime as it contains a number of provisions that establish investigation instruments but only one provision (Art. 15) that deals with safeguards, including some specific safeguards and a generic protection of "rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments..."

Another key topic and requirements for ICT related investigations is the international dimension: transnational investigations often require immediate reaction of counterparts in the country where the offender is located or data has either transited or been stored. The CoC provides a general framework for international cooperation, and in the EU this has been reinforced by instruments created by the European Commission under the Judicial Cooperation initiatives we mentioned above.

> Art. 23 CoC notes that the general principles do not only apply in investigations of cybercrimes, but in any investigation of any crimes where evidence in electronic form needs to be collected (e.g. if the suspect in a murder cases used an email service abroad).

Areas covered by this framework include;

- Extradition (art 26).
- Mutual help (art. 27): designated contact points for mutual legal assistance requests, direct communication between the contact points to avoid long lasting procedures and the creation of a database with all contact points.
- Mutual assistance regarding provisional measures (in relation to the measures set out above for criminal investigations: data retention, preservation, production, etc.).

- Transborder access to stored data.

Finally, it must be noted that significant pressure is being put on ISP (access and service providers) to cooperate and actively participate in the persecution and detection of cybercrime. While the operators themselves may benefit from exemptions of liability, these laws have also ensured and imposed obligations of collaboration with authorities and even carve-outs from exemptions when public or national security is involved.

6.7. Conclusions

Compared with private law (commercial, tort, etc.), criminal law in the ICT domain is less developed. However, most jurisdictions have implemented provisions, often deriving from the CoE Convention on Cybercrime, in their Criminal Codes or equivalent specific laws (like the UK Computer Misuse Act and others). So as regards substantive law, apart from the major areas of cultural differences there has been significant progress towards creating a harmonious international framework.

On the other hand, the Council of Europe has noted two significant problems:

- The process of implementation of the procedural law provisions, such as search and seizure, data retention – in particular regarding the conflicts with higher laws such as constitutional or international treaty safeguards of privacy.
- Obligations on ISPs and their involvement in detection and prevention.

Finally, we note that this area is one of a perpetual race between technologies used to perpetrate or hide crimes, and the same technologies used by authorities to detect (criminal forensics) and prosecute (cybercourts) crimes, on the one hand, and protect citizens and organisations on the other (cybersecurity).

Further reading

Sites:

- ITU: http://www.itu.int/ITU-D/cyb/cybersecurity/ and http://www.cybersecurity-gateway.org/legal_context.html
- Council of Europe:
- US Dept. of Justice: http://www.cybercrime.gov/

EU work:

- Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final: http://europa.eu/legislation_summaries/information_society/l33193b_en.htm

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems: http://europa.eu/legislation_summaries/information_society/l33193_en.htm

- Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005

on attacks against information systems http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0448:EN:NOT

Other:

- http://www.cybertelecom.org/security/treaty.htm
- http://www.privacyinternational.org/
- http://en.wikipedia.org/wiki/Computer_crime
- http://www.crime-research.org/
- http://www.cybercrimelaw.org/
- http://www.cybercrime-institute.com/