# THE IMPACT OF THE DIGITAL AGE ON LAW

***Mr Justice Peter Charleton and Ciara Herlihy***

When in the 1920s, radio first achieved mass penetration in the United States of America, it generated optimism on a utopian scale: the level of public discourse would be elevated; culture in sound, through classical music and drama readings, would become widespread, educating the masses; working people would be exposed to the thoughts of philosophers and experts in all fields, thereby attaining their level of reasoning; and the vast distance between the federal government and citizens would become no more than as if the entire nation was a small town.[1] When the television became popular 50 years later in the 1970s, that optimism had disappeared, criticism being the order of the day: the view was that children should be kept away from television; that exposure to low moral standards would derail society; that the excesses of pulp fiction would crowd out elevating drama, and that addiction to image would undermine the ability to work. According to Neil Postman, culture would be shrivelled through imprisonment in triviality and through turning art into a burlesque.[2] We seemed to learnt by experience. Yet, when the Internet achieved its initial burst of popularity 25 years ago, these dreams returned in an unexpected form. Many believed that a new realm had been created, one where the territoriality of nation states could not impinge with their laws and administrative controls, but where freedom, in an unfettered and pure form, would instead reign as the supreme value. Indeed, there was a declaration to that effect:

> Governments…on behalf of the future…leave us alone. You are not welcome among us. You have no sovereignty where we gather …[T]he global social space we are building [is] naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours…Cyberspace does not lie within your borders…It is an act of nature and it grows itself through our collective actions. You have not engaged in our great and gathering conversation, nor did you create our market-places…Where there are real conflicts, where there are wrongs, we will identify and address them by our means…This governance will arise according to the conditions of our world not yours. Our world is different.[3]

[1] Tim Wu, The Master Switch: The Rise and Fall of Information Empires. (New York, 2010) 38.
[2] Neil Postman, Amusing Ourselves to Death: Public discourse in the Age of Showbusiness (London 1985) 155.
[3] Peter Barlow, Declaration of Independence of Cyberspace, 1996, quoted in John Naughton. From Gutenberg to Zuckerberg: What you really need to know about the Internet (London 2012) 29.

Law applies to situations where there is a need to regulate human conduct in that sphere. Law is the pivotal point of the social compact out of which nations are constructed. Hence, law is generally territorial; it applies within the boundaries of a nation. No aspect of law is immutable. Theories of natural law may posit that values such as life are beyond regulation. Indeed, the Constitution of Ireland holds that the family is the fundamental unit on which society is based and as such possesses 'inalienable and imprescriptible rights … antecedent and superior to all positive law'; Article 41.1.1º. But, generally law is the expression of public policy. In our democratic societies, increasingly changes are proposed in public discourse where what the French call the fourth estate holds the power to swing debate, and where the touchstone of regulation is increasingly public attitudes reflected in opinion polls. Administrative inertia may leave laws in place longer than their purpose serves, but generally proposing a new law is a more difficult goal to achieve than working within the confines of existing law. Thus, whether there is a fundamental core of law apart from the Universal Declaration of Human Rights and other instruments becomes irrelevant, because the collective authority of democracy generally results in the public granting themselves that degree of regulation over those spheres which they decide need regulating. In this too, judges play their part. The accusation usually levelled by the fourth estate against the judiciary is that of being out of touch. In countries where juries try criminal cases, citizens have a judicial function. It was in the 17th century, that in England they eventually refused to return guilty verdicts on those accused of being witches. Where judges give verdicts, in the Anglo-American system, a sentence which does not reflect the crime can have the same effect as decriminalising conduct by way of judicial action; hence it becomes possible to effectively legalise brothels, drug taking, and assisted suicide in situations of extreme distress. This may be done either through verdicts or through the handing down of overly lenient penalties.

Such actions, where they occur, reflect a fundamental swing in attitude, which generally says that the law is futile. Such futility happens when acceptance of a particular wrong becomes widespread in society. This can also occur where the decision maker says that regulation of a particular matter is impossible.
Supporters of liberty on the Internet say that enforcement of the law is not welcome in that sphere. Often, enforcement is not welcome. So, that's not new. But they also call the Internet a place apart, where the law holds no sway. The architecture of the World Wide Web, coupled with experience, suggests that this may be so.

## No discrimination equals no regulation

The Internet was first developed in the 1980s in order to connect various laboratories working on defence projects in the US. Then called the Advanced Research Projects Agency Network (ARPANET), it was extended to enable communication between laboratories in order to bypass printing and travel. Since the terminals and login procedures differed, and since it was impossible to get various sets of computers to use a common communications language, the solution that emerged was the interposition of a set of computers as interface. Thus, each set of computers would be interacting with the Interface Message Processor, and the IMP became central to the design. There remained the problem of an interface which would link networks that were not centrally controlled and which passed material that could not be predicted; text, voice telephony, chemical formula, images. The solution was:

1. that there should be no central control over the network;
2. that the network should not be optimised for any particular application but should, instead, be maintained in the simplest possible state to enable computer to computer communication in respect of every form of material;
3. that the form of the data packets should be specified, but that there should be no control over the content;
4. that data packets should be sent and received in their intended order, in strings of data, so that linked together by code, they would assume the form in which they were intended.

Thus the Internet simply takes material, the packets, in at one end and delivers them to the other. Since what it is carrying is digitised, this can be a set of data, music, video or images. All of these can be expressed in packets and linked through code.[4] The modality is to find the best way for A to communicate with B and to bypass blockages. The Internet was therefore built on open, permissive architecture and since there was no central control, it could not specify who could participate or block any network from joining. In that respect, it is radically different from radio and television and was especially different from government-controlled agencies. Enormous effort is required to block access to the Internet, as with what is called the Great Firewall of China.[5] Personal communications from China indicate that even this can be bypassed with the correct tools. The basic protocols of the Internet are designed to find ways through anomalies in communication in order to deliver data.

[4] Naughton, 43-58, 297-306.

[5] Andrei Soldatov and Irina Borogan, 'Putin brings China's Great Firewall to Russia in cybersecurity pact', The Guardian, 29 November 2016 (https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact).

The Internet is fully international. An application in a particular country can potentially be accessed in any other country, and the location of that access can be disguised by rerouting data through various servers in order to give a misleading impression. Particularly large firms discovered early in this century that not all of the vast space on their servers was being taken up at any particular time and that therefore there was a way of using that extra space to attract customers. Since the unique data code on packets linked them together, these could be stored offsite in what has now become known as the cloud.[6] The invention of cookies, whereby most commercial servers may place text files on the customers' computer when their site is accessed, has allowed companies to know which computers have previously accessed their site. For example, in booking a Ryanair flight, the customer must click on a box which indicates agreement with the terms and conditions of booking. That is not done on the Ryanair server, rather the Ryanair server has placed a placed a program on the customer's computer which then signals to the commercial server agreement with the question asked. It is the customer's computer which will not allow further access to the Ryanair site unless that box is ticked.[7]

The growth and expansion of the World Wide Web has been phenomenal. There must be something in human nature which compels people to seek to be noticed. Every minute, 48 hours of video, personal and also often copyright owned, but often forgotten, like old films or TV clips, are added to YouTube. It is estimated that close to one third of the world's population have access to the Internet.[8] If you have a product or service to offer, your marketplace is incomprehensibly larger thanks to the Internet. We have moved over human history from having a local village marketplace, to a city marketplace, to a national marketplace through radio and television, to literally having the world as the place to sell and buy. For legal and illegal purposes, access to the Internet is both cheap and easy. The Facebook story is the illustrative one, and its popularity is clearly evident on a global scale.[9] Initially a website within the Harvard University network for rating the attractiveness of girls on campus, this sexist network was rightly shut down by the college's firm disciplinary rules. However, because it generated 22,000 hits over a few days, the viability of a social networking site linking leading American universities became apparent. A group of friends built the site into one for social interaction. The Internet being neutral, open and free, the natural growth of an elite Ivy League university networking website into a worldwide phenomenon

[6] Cloud storage services are 'global storage facilities [used] to store information electronically and grant access to uploaded information using any electronic device from any location at any time.' Laurie Buchan Serafino, 'I Know My Rights, So You Go'n Need a Warrant for That' The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds, (2014) 19 Berkeley Journal of Criminal Law 154, 161

[7] Naughton, 210. See also Patrick Collinson, 'Beware the cookies: they can cost you money', The Guardian, 7 August 2010 (https://www.theguardian.com/money/blog/2010/aug/07/computer-cookies-booking-online)

[8] International Telecommunication Union, 2016 Press Release ICT figures show that 3.9 billion people do not have access to the internet (http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx).

[9] Facebook attracted an average of 1.23 billion daily active users in December 2016. Facebook 2016 stats, (https://newsroom.fb.com/company-info/).

backed by the continuous development of new services and superb technical implementation, generated 600,000,000 users. The initial cost for the web design was less than $1,000 and in the initial phase, web hosting cost $85 a month up to the point where Facebook had 250,000 users.[10]

To even ask if criminals use the internet to their benefit is idiotic! It is claimed that the Dark web was developed in the US by security agencies.[11] Not accessible by ordinary search engines, downloading programmes such as the Tor browser will enable the widest possible range of truly vicious criminal services to be available. Nearly all paid for in cryptocurrency such as Bitcoin, while anonymity is not guaranteed and while every website accessed by an individual user leaves a trace somewhere, investigations become extremely difficult. People can hide in cyberspace. In the centre of Dublin, over a 10 year stretch a man called Eric Eoin Marques, claimed by the FBI to be 'the largest facilitator of child porn on the planet', operated without detection. He was arrested in Dublin in 2013, however the DPP decided to not prosecute him for child pornography offences. Marques was wanted by the US authorities to face charges in that jurisdiction, and lost a challenge to his extradition to the US in the Court of Appeal in December 2016.[12] An investigative journalist who recently explored the Dark web found websites offering the sale of a high quality European passport, an unused handgun and pure Peruvian cocaine, all of which were available to purchase in a few clicks.[13] This is shocking.

One such website where drugs and guns could be purchased was Silk Road, created in 2011 and run by a young science graduate Ross Ulbricht. Described by US Senator Chuck Schumer as a 'certifiable one-stop shop for illegal drugs',[14] US authorities initially found it impossible to shut down the website, where individuals traded in Bitcoin. Within a year, $500,000 a month was being generated in drug sales, on which Ulbricht made a 6% commission, and this only continued to increase as guns and forged passports also became available for purchase.[15] Ulbricht was tracked down and arrested in October 2013, and given a life sentence without parole in May 2015, convicted of a number of offences including the distribution of narcotics, computer hacking and money laundering. As the prosecution argued prior to sentencing, Ulbricht's offences warranted a severe penalty as '[he] did not merely commit a serious crime in his own right.

[10] Ben Mezrich, The Accidental Billionaires: Sex, Money, Betrayal and the Founding of Facebook (New York, 2010).
[11] Jake Wallis Simons'Guns, drugs and freedom: the great dark net debate', The Telegraph, 17 September 2014 (http://www.telegraph.co.uk/culture/books/11093317/Guns-drugs-and-freedom-the-great-dark-net-debate.html)
[12] *Marques v DPP* [2016] IECA 373. 'Man loses extradition challenge in child abuse images case', RTÉ, 12 December 2016 (https://www.rte.ie/news/2016/1212/838362-eric-eoin-marques/).
[13] Adam Cullen, 'Inside the dark net: Guns, drugs and hitmen are just a click away', Irish Independent, 29 August 2015 (http://www.independent.ie/irish-news/news/inside-the-dark-net-guns-drugs-and-hitmen-are-just-a-click-away-31486739.html).
[14] As quoted in Ben Popper, 'Chuck Schumer Bashes BitCoin, Wants to Shut Down Silk Road Drug Site', The Observer, 6 June 2011 (http://observer.com/2011/06/chuck-schumer-silk-road-bitcoin-drugs/).
[15] Nick Bilton, 'Silk Road to Riches – And Ruin', The Sunday Times Magazine, 30 April 2017

He developed a blueprint for a new way to use the Internet to undermine the law and facilitate criminal transactions'.[16]

## Obscenity as a paradigm

At the foundation of the State in 1922, in Ireland and in Great Britain, the common law made it a crime to publicly expose the naked person or to publish obscene material. The test for obscenity was whether the tendency of the matter charged as obscenity was to deprave and corrupt those whose minds were open to such immoral influences and into whose hands the publication of this sort would fall.[17] While there is a danger of being po-faced and prudish when dealing with this matter, insofar as anyone has tried to keep up-to-date with any attempt to protect the young, the Internet has made a vast range of material easily available on mobile phones and laptops. Unfortunately, the nature of the pornography industry shows a natural tendency towards deeply degrading practices of which it then becomes an evangelist.

If this is a problem, and if it is not the case that the law has become dead by universal breach, then the scale of what is faced becomes apparent. In the documentary film *Hot Girls Wanted*,[18] we learn that more people visit porn sites each month than Netflix, Amazon and Twitter combined. In the US, thousands of 18 to 20 year old girls enter the porn industry each year. The comment is that the person playing 'the girl next door' role has become the girl next door. The universal nature of the Internet means that regulation in one country aimed at preventing the exploitation of young people means that the industry only has to cross the border to avoid any well-intentioned law. For instance, California recently passed a law requiring the use of condoms in pornography and this led to Miami becoming popular for filming as it does not have an equivalent law in place. Girls shoot about 3 scenes per week, typically earning $800 a scene. They are lucky to last 6 months in the industry, replaced by the next girl who comes along, and one young woman taken as an example went home with only $25,000 out of earnings that were many multiples of that. According to the documentary makers:

> Twitter is key to an aspiring porn star's success. Unlike Facebook and Instagram it does not censor most porn content. The minimum age to have a Twitter account is 13.

[16] *USA v Ross Ulbricht* 14 Cr. 68 (KBF), Government sentencing submission, https://cryptome.org/2015/05/ulbricht-256.pdf, 13

[17] John Frederick Archbold, Pleading, Evidence and Practice in Criminal Cases, 26th ed London, 1922) 387.

[18] 2015, directed by Jill Bauer and Ronna Gradus. A curious feature of this rightly polemical film was that more girls applied the year after it delivered its warnings than before to join the porn network.

US law requires girls to prove they are at least 18 years old on entering the industry, but no other regulations have been adopted in this context.[19] Freedom of expression under the US Constitution was the basis for the Supreme Court striking down parts of the Communications Decency Act 1996 in *Reno v ACLU*.[20] The Act made it a criminal offence to knowingly use the internet to send sexual content or to display such content to a person under 18. It may be that freedom of expression is a good thing, and indeed it is, but perhaps it should have limits:

> 'Teen' is the number one searched item in Internet pornography. A popular trend in porn is the forced blow job. Sites like 'Facial Abuse' feature extreme oral sex aimed at making a girl vomit. In 2014 abuse porn websites averaged over 60 million combined hits per month. More hits than nfl.com, nba.com, hotwire.com, cbs.com, fortune.com, Disney.com, nbcnews.com.[21]

Perhaps we need to recast the law? Who is the victim here? Surely it is young women? Obscene, in a more modern age, might be redefined as to whether the depiction of an action degrades the person to whom it is done. After all, was not this kind of conduct a form of slave degradation, with payment merely incidental? In Great Britain, the Digital Economy Act 2017 tightens up access by young people to particular sites and bans particular forms of sexual conduct being depicted on screen.[22] The Act, which received royal assent on the 27th April 2017, was met with predictable opposition, the argument being that 'adults should be enabled to view adult content.' David Kaye, United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression described any such move as giving to government 'access to information of viewing habits and citizen data', as 'eradicating anonymous expression, one of the most important advances facilitated by the Internet', as lacking 'judicial oversight' and as falling 'short of the standards of international human rights law.'[23] This is a point of view: but is it right? What human rights is he talking about?

## Ireland

The creation of computers as a medium evoked at least one early Irish response. This was in the Criminal Damage Act 1991, s.5 of which made it an offence to

[19] Hot Girls Wanted, 2015
[20] 521 US 844 (1997)
[21] *Hot Girls Wanted*, 2015.
[22] Damien Gayle, 'UK to censor online videos of 'non-conventional' sex acts', The Guardian, 23 November 2016 (https://www.theguardian.com/technology/2016/nov/23/censor-non-conventional-sex-acts-online-internet-pornography?CMP=twt_gu).
[23] Damien Gayle, 'UN free speech advocate criticises UK plan to curb access to online porn', The Guardian, 12 January 2017 (https://www.theguardian.com/technology/2017/jan/12/un-free-speech-advocate-criticises-uk-plan-curb-access-online-porn)

'access any data kept either with or outside the State' or access data 'kept within the State' from 'outside the State'. The maximum penalty is 3 months' imprisonment, which in the light of the severe damage computer hacking can do, may be inadequate in some cases.

The Irish response to the copyright problem, whereby music and video files were being downloaded and shared, without fee, was to issue injunctions against Pirate Bay and cognate sites. More controversially, the High Court decided in principle in favour of a graduated response towards those illegally downloading copyrighted material, a matter to be enforced through the service provider; *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd*.[24] This has engendered a vast debate on the appropriate response to illegal downloading and could, in itself, be regarded as a second paradigm. Many in the music industry say that a generation has grown up who do not believe in paying for music. It is only this year, however, that the commercial response to this problem in the form of music subscription services, which pay artists for their work, have finally outpaced the sale of music in hard formats. If you talk to anyone in the music industry, however, they will say that the amount of compensation has dramatically dipped and unless a rock group is at the very top level, being a full-time musician has become next to impossible.[25] Effectively, the existence of the Internet has fundamentally undermined protection for copyright. One may take the view, along with John Naughton, that this is another instance where reality has to kick in. Nothing will ever stop these activities, so the responses should be professional, in the sense of providing what consumers want at a reasonable price, or administrative. Those administrative measures could very rarely justify even a graduated response enforced through a service provider. Copyright has become one of several competing rights in European law, and the alternative and contending rights include the right to anonymity over the Internet, a curious taking up of the torch of Internet liberty, the right to earn a livelihood, to communicate, and the right to legal and medical assistance. The issue then becomes about where the balance lies; European Court in *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.[26]

In terms of law reform, both the Oireachtas (National Parliament) and the Law Reform Commission, have issued detailed reports in this context. These favour

[24] [2010] IEHC 377, (Unreported, High Court, Charleton J, 11 October 2010). See also *EMI Records (Ireland) Ltd v Eircom plc* [2009] IEHC 411, (Unreported, High Court, Charleton J, 24 July 2009) on the grant of an injunction against the defendant Internet service provider to block access to Pirate Bay, later declared to be incorrect in *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd*; and *EMI Records & Ors v Eircom Ltd* [2010] 4 IR 349 upholding the validity from a data protection perspective of the three strikes and cut-off settlement as between the parties. It is understood that on 5 December 2011, the Irish Data Protection Commissioner issued an enforcement notice directing Eircom to stop implementing the agreement. The matter is now before the commercial division of the Irish High Court. See Mary Carolan, 'Music firms in data legal challenge', The Irish Times, 29 February 2012 (http://www.irishtimes.com/newspaper/breaking/2012/0229/breaking39.html).

[25] Personal communications. See also Elle Hunt, 'Judge orders internet providers to block illegal downloading websites', The Guardian, 15 December 2016 (https://www.theguardian.com/technology/2016/dec/15/judge-orders-internet-providers-to-block-illegal-downloading-websites).

[26] Case C-70/10, 24 November 2011

platform neutrality; the idea being that special laws for the Internet may be seen as an attack on that platform: consequently, the favoured approach is one of prohibition in a general sense. Thus, to give an example, it is illegal to import drugs but it is not specifically a crime to use the Internet for the purpose of obtaining contraband. The approach considered best is to legislate for gaps which have been exposed by the Internet, but to do so in a way which addresses the problem rather than the platform itself. Both favour administrative measures, or civil responses, and the Report of the Law Reform Commission on Harmful Communications and Digital Safety applies proportionality, stating that the hierarchy of responses in the context of internet regulation should be one of education, civil law or regulatory oversight and finally criminal law:

> With regard to proportionality, this Report applies the harm principle, which requires that responses based on policy, education and the civil law should be prioritised and that the criminal law should only be employed to deal with serious harm. The Report therefore recommends a three level hierarchy of responses to target harmful digital communications…[27]

Even abiding by the principle of platform neutrality, it is clear that social media and social networking websites have caused an explosion in the potentiality for bullying and harassment. It is common among the younger generation to send explicit photographs and videos, known as sexting, and these may be shared with others as a means of revenge when, as is inevitable, the majority of these relationships do not work out. While, again, the right to freedom of expression may be posited as a bar to any legislative action, the right to privacy also exists. It is fair to imagine that the normal human distinction between what is privately shared with a friend and the sense of betrayal which comes if that is broadcast to the nation, also applies in the context of intimate relationships if material is later shared with the public through a digital medium.[28] Thus, the proposal is to repeal section 10 of the Non-Fatal Offences against the Person Act 1997 and to enact a new offence to include harassment done by any means of communication; to enable prosecutions for stalking through a digital medium; to address once-off harmful communications because of the grave damage that these can do; to make it an offence to send or threaten to send intimate messages, whether once off or otherwise; and to criminalise upskirting. Obviously, with the international element involved in online communications, this will require extra-territoriality to apply in the context of the new offences proposed, in terms of origin and in terms of methodology. The newly proposed offences may also intersect with hate crimes online to some extent. If Ireland ratifies both the Council of Europe Convention on Cybercrime and the Additional Protocol to the Convention, this

[27] LRC 116-2016 at 4.

[28] Facebook moderators, for example, escalated some 51,300 reported cases of revenge porn to senior management in January 2017, Nick Hopkins, 'Facebook flooded with sextortion and revenge porn, secret files reveal', The Guardian, 23 May 2017

would lead to reform of legislation to criminalise acts of a racist and xenophobic nature perpetrated through computer systems.[29]

While there are many quangos, it seems correct that the Law Reform Commission proposed to establish a Digital Safety Commissioner who would oversee service providers. In this way a remedy would be provided whereby a complaint could be verified and swift action could be taken requiring the service provider to take action. This, as may be seen later, conflicts with a basic principle of European legislation, but one that is increasingly under attack. The proposal would go so far as to enable that official to apply to the Circuit Court for an order requiring compliance; the defiance of which would, of course, amount to a contempt of court.[30]

**France**

While in Ireland, ISPs operate a practice of self-regulation, guided by a code of practice and ethics; in France, a number of measures have been introduced to regulate the internet in the context of intellectual property and access to child pornography and pro-terrorist websites.[31] The well-known HADOPI law was introduced in June 2009,[32] establishing a government institution to deal with the protection of copyright and the circulation of artistic works online. Given the increasing problem of illegal downloading, it also attempted to promote legal access to artistic works.[33] This law applies the principle of graduated response. A person may complain that an internet user has illegally accessed material that they hold rights over, and the internet user can be issued with a warning where their IP address is identified. The maximum penalty for failing to comply with HADOPI warnings is now a €1,500 fine. An amendment to the law in 2013, however, removed a court's ability to suspend an individual's internet access where they had failed to comply with numerous HADOPI warnings.[34] This is the ultimate penalty.

LOPPSI 2, enacted in March 2011, was a further attempt at legal regulation of the internet in France.[35] The Conseil Constitutionnel found that 13 articles of the 142 measures in the original bill were unconstitutional,[36] however the more significant provisions such as Article 4 were upheld. This allows administrative

[29] LRC 116-2016 at 117.
[30] LRC 116-2016 at 11.
[31] See further on the use of the internet and social media to spread pro-terrorist content, Nick Hopkins, 'Facebook's 'impossible' battle to control flood of content that glories extremists', The Guardian, 24 May 2017, which reports that Facebook's content moderators identified over 1,300 credible terrorist threats on the site over the course of one month in 2016.
[32] Loi no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet
[33] HADOPI runs a website which lists creative works available free and legally online: www.offrelegale.fr
[34] This had been originally been inserted by Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, and was removed by a decree n° 2013-596 du 8 juillet 2013.
[35] Loi no 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
[36] Décision n° 2011-625 DC du 10 mars 2011

authorities to require an ISP to block access to certain websites, if they are of the view that this will prevent the distribution and display of child pornography.

More recently, in 2015, two decrees were adopted into French law. The former Minister for the Interior, Bernard Cazeneuve, considered that terrorism could not be fought against without regulating the internet, and that, in this context, legal regulation did not constitute an attack on the freedom of expression.[37] Is freedom of expression an absolute value, after all? The first decree allows access to pro-terrorist and child pornography websites to be blocked.[38] The ISP has 24 hours to block access, and where a website is blocked, an internet user who attempts to visit this website will be redirected to the webpage of the Minister of the Interior. A central office has been established in French police tasked with fighting against cybercrime, which must check blocked websites at least four times a year.[39] A website may be unblocked if the original illegal content no longer remains. In March 2015, French media reported that five pro-jihad websites had been blocked under the decree.[40]

The second decree allows pro-terrorist or child pornography websites to be removed from internet search engine results.[41] The office similarly identifies these websites and must also review the removal on a quarterly basis to ensure that grounds remain for the removal.

Opponents of these measures have criticised the lack of judicial oversight in blocking access to websites and argue that these measures represent a disproportionate infringement on freedom of communication, undermine the freedom of speech and constitute internet censorship.

## Great Britain

Known as revenge pornography, the distribution of intimate images without a person's consent is one area which has attracted considerable legislative attention in recent times. In 2015, the distribution of sexual photographs and films with intent to cause distress became a criminal offence under the law in England and Wales under section 33 of the Criminal Justice and Courts Act 2015 with a maximum penalty of two years' imprisonment. A number of defences, such as disclosure of images for the purposes of preventing, detecting or investigating

[37] UK Prime Minister Theresa May recently made similar comments regarding the need to suppress extremist content online, see Anushka Asthana, 'May: technology giants must lead fight against extremism', The Guardian, 26 May 2017

[38] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

[39] OCLCTIC (l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication)

[40] Amaelle Guiton, 'Cinq sites web projihad bloqués de l'Intérieur', Libération, 16 March 2015 (http://www.liberation.fr/ecrans/2015/03/16/cinq-sites-web-projihad-bloques-de-l-interieur_1222042)

[41] Décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

crime, are also outlined in the section.[42] Equivalent legislation was introduced under section 51 of the Justice Act (Northern Ireland) 2016. Scottish law also recently enacted an offence of 'disclosing or threatening to disclose an intimate photograph or film' under the Abusive Behaviour and Sexual Harm (Scotland) Act 2016.

This type of behaviour does not constitute a specific criminal offence under Irish law, although the Law Reform Commission as mentioned above has recommended that a specific criminal offence be created along the same lines as UK legislation in this context.

**United States of America**

The First Amendment to the US Constitution states that Congress 'shall make no law … abridging the freedom of speech'. This clearly places limits on the extent to which the legislature may interfere with freedom of speech online in order to regulate the internet. In the late 1990s and early 2000s, Congress sought to regulate the internet and more specifically regulate young peoples' access and exposure to sexual content online. Violation of First Amendment rights was the basis for the US Supreme Court striking down the anti-indecency provisions under the Communications Decency Act 1996 in *Reno v ACLU*, the court finding that the Act placed an unacceptably heavy burden on constitutionally protected speech.[43] Section 230 of that Act is a significant provision however which remains in effect. It provides that '[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'. Effectively, this creates an immunity, similar to that in European law, from liability for hosts such as social media websites for content published by an individual user of that website. A 'safe harbour' provision is also included in the Digital Millennium Copyright Act 1998 which limits the liability of ISPs for copyright infringement by internet users.[44]

Further attempts to regulate the internet in the US have been met with opposition in light of the constitution protection given to the freedom of speech. Following the *Reno* case, the Child Online Protection Act 1998 was passed, but never took effect as it was subject to numerous legal challenges. The Act made it an offence to knowingly communicate obscene material harmful to minors. The Third Circuit Court of Appeal in *ACLU v Mukasey* upheld a previous finding of unconstitutionality[45] and the Supreme Court refused to hear a further appeal,

[42] Other defences are the disclosure of such material in the course of, or with the view to, the publication of journalistic material where the individual believed this disclosure was or would be in the public interest, and disclosure where the individual reasonably believed that the material had been previously disclosed for reward.
[43] *Reno v ACLU*, 882
[44] Section 512, Title II- Online Copyright Infringement Liability Limitation Act (OCILLA)
[45] No 07-2539, 22nd July 2008

meaning that enforcement of the Act continued to be blocked. This was described by the ACLU as a victory for online free speech.[46] Indeed it may be, but are there not other rights involved as well?

The Children's Internet Protection Act 2000 was upheld as constitutional by the US Supreme Court in 2003. It required public schools and libraries, as a condition of state funding, to use internet filters in order to prevent children accessing obscene material online. The Supreme Court found that this did not violate First Amendment rights.

**Germany**

A new bill has recently been introduced by the German cabinet, known as the Network Enforcement Bill (*Netzwerkdurchsetzungsgesetz*).[47] The Bill places greater obligations on popular social networks such as Facebook and Twitter in terms of how they deal with complaints of unlawful and illegal content on their websites.[48] The Bill requires these service providers to publish a quarterly report on how the website has handled user complaints, and the Bill seeks to regulate the manner in which these websites deal with user complaints in outlining the steps to be taken by them. This includes an obligation to speedily acknowledge the complaint and assess whether the content complained of is unlawful, and delete clearly unlawful content within 24 hours. Any content which is not clearly unlawful on its face must be examined and deleted within 7 days if found to be unlawful. The host website must inform the parties affected of the decision, giving reasons for the removal or non-removal of content. Social networks may face fines of up to €5 million for failure to provide an effective complaint mechanism for users and failure to report on handling of complaints. While social media sites have their own procedures for dealing with user complaints, the Bill places heightened obligations on websites in providing a specific mechanism under which user complaints are to be dealt with as well as a reporting obligation.

Many predict the Bill will be challenged, and indeed the rumblings against it have a familiar tone. If so the ultimate limits of authority between legitimate protection and freedom of expression will be delineated by the Bundesverfassungsgericht.

---

[46] ACLU, 'In Victory for Online Free Speech, Supreme Court Upholds Block on Internet Censorship Law' (https://www.aclu.org/news/victory-online-free-speech-supreme-court-upholds-block-internet-censorship-law)

[47] Martin Gerecke, 'Germany: new bill obliges social media networks to monitor and remove certain unlawful content', 28 April 2017 (http://www.lexology.com/library/detail.aspx?g=e2c6fb48-4a15-4797-8e54-d891cf7419e3)

[48] See Nick Hopkins, 'Revealed: Facebook's secret rules on sex, violence, hate speech and terror', The Guardian, 22 May 2017, detailing the Guardian's access to over 100 internal Facebook documents which outline the website's policies for moderating content. However many critics of Facebook's policies are of the view that the site should be regulated in a similar manner to mainstream media companies and broadcasters. Facebook currently employs an estimated 4,500 content moderators worldwide.

## New medium a sharpened danger

A problem has to be faced. The Internet has provided a new platform of unfathomable power over which communications can move, at least in theory, at the speed of light. Consequently, where once a nasty anonymous letter might be sent to one person and cause some harm to that individual, the sharing of intimate photographs may now be communicated without thought and with little reason to the entire world in an instant. The Internet is a sharpened danger and it is foolish to ignore its potentiality for harm, while we can also acknowledge the massive act of generosity that many sites such as Wikipedia represent. Since the Internet consists of a set of linked computers, it is the routers for the data packages that have traditionally been the subject of legal focus. While it may be impossible, or unreasonable, to pursue individual perpetrators, those who have Internet connection, in practical terms, have to pay a subscription to a provider. It is clear, also, that with the billions of connections that take place every day through these networks, providers cannot be expected to police every page and every line of every text and every photograph or video.

## The mere hosting defence

The E-Commerce Directive provides Internet service providers with specific defences to claims of copyright infringement.[49] The 'mere conduit' defence in Article 12 arises when the Internet service provider does not initiate the transmission; does not select the receiver of the transmission; and does not select or modify the information contained therein. Article 13 provides a defence where the Internet service provider is merely caching information or websites, for instance to enable more ready access to popular search terms; and Article 14 provides a defence in circumstances where the Internet service provider is merely hosting information or websites. Further, Article 15 prohibits member states from imposing a general obligation on Internet service providers to monitor the information which they transmit or store, and in appropriate circumstances they may be able to argue that the mere provision of facilities for enabling or making a communication is neither a crime nor a civil wrong, such as a breach of copyright.[50]

Clearly, to avail of the mere service provider defence in Article 14, it is necessary to examine what exactly was done by the service provider and the defence seems only to be available in neutral circumstances 'in the sense that its conduct is

[49] 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
[50] Directive 2001/29/EC (the Copyright Directive), Recital 27.

merely technical, automatic and passive, pointing to a lack of knowledge or control of the data it stores'; *Google France v Louis Vuitton.*[51]

Increasingly, it has fallen to the European Court of Human Rights to balance the right to privacy against the right to freedom of expression within this context. Some have seen a shift in favour of upholding the right to privacy. In *Von Hannover v Germany,*[52] the Court upheld the claim that failing to provide a remedy for photographs taken in a public place without consent constituted a breach of Article 8 of the European Convention on Human Rights, which guarantees the right to privacy in family and personal matters. The touchstone may be as to whether what is published is of 'general interest' and where no such contribution is made, the contending right to freedom of expression may fail. In *Delfi AS v Estonia,*[53] an online news portal was held liable for comments generated by a user. Four factors were identified as being relevant for analysis by the Court: the context of the comments; whether the poster as opposed to the service provider might be found liable as an alternative; what was done by the service provider to prevent or remove the defamatory comments; and the consequences.[54] It would be possible in the light of 'the rights and interests of others and of society as a whole' for countries to impose liability if service providers 'failed to take measures to remove clearly unlawful comments without delay'. [55] Perhaps the analysis went too far in saying that this was possible 'even without notice from the alleged victim or from third parties', [56] since this places an intolerable burden on service providers and is unrealistic. The case of *Magyar Tartalomszolgátatók Egyesülete v Hungary*[57] represents a pulling back from that extreme position in favour of restricting liability which 'may have foreseeable negative consequences on the comment environment of an Internet portal', a comment which indicated the court's desire not to have 'a chilling effect on the freedom of expression on the Internet'.[58]

It is not surprising, therefore, that the Law Reform Commission describe the balancing of these contending rights as 'a challenging task, particularly in the digital and online context.'[59] They therefore did not propose any 'heavy handed law based measures'[60] but instead comment:

> The best approach may be to prioritise less coercive solutions such as policy and education based remedies as well as civil law solutions.

[51] Cases C-236/08, C-237/08 andC-238/08, para 114.
[52] [2004] EMLR 21.
[53] (2014) 58 EHRR 29.
[54] *Delfi AS*, para 64
[55] *Delfi AS,* para 159
[56] *Delfi AS,* para 159
[57] Application number 22947/13, 2 February 2016
[58] *Magyar Tartalomszolgátatók Egyesülete,* para 86
[59] LRC 116-2016 at 38
[60] LRC 116-2016 at 38

> However, it is important that criminal laws are in place to deter especially harmful behaviour and ensure that appropriate responses are available for the most serious cases.[61]

**Where the law might go**

In some instances, the practical consequences of the medium that the Internet represents has had the effect of placing legal responses almost outside the scope of what is practical. The two paradigms mentioned here, of obscenity and of copyright infringement, both demonstrate the shifting nature of the medium when it comes to framing any remedy. In the context of copyright, many, such as John Naughton, believe that the only response has to be a commercial one which takes into account the reality that the Internet has caused a generation of consumers to be lost and copyright undermined in favour of the freedom of expression and online anonymity. Others will continue to fight the battle on the basis that payment for creative endeavours is also a noble cause. There may be some circumstances where the washing of hands or wringing of hands might be a disavowal of the government's duty to establish social order.

Were any restriction to be posited on freedom of expression, in the context of obscenity, objections would be made against the paternalistic regulation of the adult world. This perhaps ignores, however, facts which make that clarion ring somewhat hollow. Every sane person agrees that children have to be protected and that child pornography exploits the vulnerable in a way which can leave a lasting mark on their personalities, perhaps over a lifetime. Real harm is being effected over the Internet. In light of this, there have to be circumstances where the argument that legal remedies, such as prosecution, have no effect because of a disproportionate interference with Internet freedom do not hold sway. While the Internet may trick us into believing that the digital world is an unreal alternative parallel universe, it is inputted only by human beings, and through the creation of saleable material by human activity. The law has always regarded particular forms of human activity as being obnoxious to social order as they undermines the fundamental right of people to live in peace and security. Many ideas, such as that of obscenity, have been challenged as to their validity in the digital age. Perhaps such concepts need to be re-calibrated in the context of the overarching aim of legal systems to protect the dignity of the individual.

While the cry has certainly gone up for freedom on the Internet, to the effect that it be made a law-free zone, the medium is not the message. Thus, to organise a murder over the Internet or to organise the importation of firearms online remains a crime regardless of the medium used. Consequently, legal regulation which is outdated, for instance in relation to harassment, should be

[61] LRC 116-2016 at 39

subject to the same updating required of the Offences against the Person Act 1861 when the prohibition on threatening to kill someone 'in writing' became neutralised by the inclusion of a threat made 'by any means' under the Non-Fatal Offences Against the Person Act 1997. Insofar as new forms of intimidation and degradation have increased in scope through instant communication and worldwide availability, while remaining neutral, legal prohibitions may be needed to address an old problem which has emerged in a new format.

Sensibly, the Law Reform Commission have identified that the pressing need exists for a new public official to act as an intermediary between the virtually powerless citizen and the muscular commercial power of Internet service providers. While in Ireland, their conduct has been self-regulated through a code, if legal practice has demonstrated anything, it is that cases slip through the cracks and that is particularly so for the disadvantaged and financially challenged who may be unable to access the court system. Increasingly it is the case that a sensible public official ultimately having resort to the courts is of the best financial value, and the lower trial courts may provide remedies which have become necessary in the digital age.