European Committee on Crime Problems

Strasbourg, Tuesday 10 June 2014

The legal and behavioural impact of modern technologies

Yves Charpenel*, premier avocat général* at the *Cour de cassation*

The introduction of so many technologies is tending to give rise to behavioural effects which lead to the adoption of new laws to deal with them. Those laws in turn may have an effect on behaviour, the extent and detail of which cannot always be predicted.

The digital revolution sweeping through our 21st century societies, while of course rooted in the technological innovations of the second half of the 20th century, is unprecedented in terms of its speed and worldwide scope, thus presenting lawmakers worldwide with a major challenge of trying to strike a delicate balance between the area of freedom opened up to all by these new technologies and the rules and regulations which need to be put in place so that our democracies are not rendered impotent.

Science without conscience is but the ruin of the soul, according to François Rabelais, that great Renaissance humanist, and the triumph of the cyber-world illustrates the currency and acuity of that principle. People's appetite for technological progress is always greater than the caution advocated by behavioural scientists, and cyber-criminals always move faster than the cyber-police.

Cybercrime remains first and foremost a crime, and Internet freedom does not exist to deny all the rights, won at such great cost, enshrined in international conventions. Viewed from France, a country where the law is set out in writing, there is nothing rhetorical about the question of the legal and behavioural effects of new technologies. Assessing those effects is made even more difficult by two interacting tendencies.

One is the profusion of rules and regulations which may prove off-putting to legal experts and ordinary people faced with the legal dimension of the new technologies:

International rules and regulations first, where, since the November 1995 European Union Directive on personal data protection and the Council of Europe Convention on Cybercrime adopted in Budapest in September 2001, there has been a succession of reference texts.

In France, there has been a stream of legislation since the law on personal data files, of 6 January 1978, up to the very recent law on geolocation, of 28 March 2014, not forgetting laws such as that of 21 June 2004 on confidence in the digital economy, that of 6 August 2004 on the protection of individuals in respect of personal data processing, that known as the HADOPI law of 12 June 2009 on creation and the Internet, and that of 12 May 2010 on on-line gambling: every year brings a new crop of legislation making it even more problematic to apply the principle on which our law is founded: the law is presumed to be known by all.

The other is the breakneck speed of developments in technology and in the services commercially available.

The wave of technological developments meets a simple response from consumers, citizens, persons subject to the jurisdiction of the courts: they adopt every innovation and freely test every possibility, moving from Internet 2.0 to cloud computing as disarmingly easily as they adopted e-shopping and started filing their tax returns on line.

There are **two kinds of reactions** amongst legal experts, and these come to complement and fit in with each other as time goes by. Firstly, **long-established legal responses** are applied to the new subject. As is the case in crime matters when appraising the fairness of evidence (I refer you to the *Cour de cassation* judgment concerning an FBI website and to the French Wikipedia website on geolocation, entitled *géolocalisation*). Also in matters relating to the protection of privacy, where the long-established rules of Article 1382 of the Civil Code or of the 1881 law on the press are applied.

Secondly, **training tools and regulatory bodies are developed**, with in-service training for members of the judiciary being introduced five years ago, and recommendations being made in the interministerial reports of June 2014.

To illustrate this triple movement, combining, sometimes in a disorderly way, the turning of technological innovations into products of mass consumption, new kinds of social behaviour which outlast fashion, and the adoption and application of ad hoc legislation, we shall consider four examples which seem to encapsulate this fast-moving area:

1. Crime

Both in everyday terms and at the level of international organised crime, the pattern is the same: a new tool, such as the mobile phone or the Internet, prompts criminals to spring into action.

Unless there are appropriate legislation, a crime policy that is applied and international co-operation, disorder prevails. In the **everyday criminal world**, both “happy slapping” and the “selfie after sex” are in fashion. The impact of the law on crime prevention of 5 March 2007, which deals specifically with violent images, shows that reactive legislation can be effective.

Where organised crime is concerned, the **trafficking of human beings via the Internet** has proliferated, enabling criminals to find victims and customers and to launder money securely on line. A colloquy on this subject was held at the National Assembly on 13 March 2014 by the Fondation Scelles, looking at the best and worst aspects of the digital society (entitled *Société numérique, du meilleur au pire*).

There are reasons for hope:

New technologies sometimes generate their own **antidotes**, with cyber-vigilantes watching out for child pornography and terrorism, and with tablets being geolocatable.

Long-established law sometimes brings appropriate responses, as when case-law recognises national jurisdiction over any offences spread via the Internet.

2. Intellectual property rights

The counterfeiting world has been hit by the use of new technologies, and particularly the **on-line sale** from one country of goods prohibited in another. The eBay judgments of 3 May 2012 denied eBay the more protective status of hosting service provider.

While the MEDICRIME Convention has, since 2010, offered appropriate tools against the counterfeiting of medicines, the question of **illegal downloading** largely remains open, notwithstanding the adoption in June 2009 of the HADOPI 1 law on prevention and in October 2009 of the HADOPI 2 law on enforcement.

A huge amount of work is being done. Three million warnings have been issued since 2010, 100 reports have been made to the prosecution service, and 17 Internet users have been convicted of offences.

3. The law on the press and personal data

The press has undergone widespread digitisation, and a French law passed as long ago as 1881 guaranteed its "freedom to print". The global and instantaneous nature of publication has had far-reaching effects on press law and practice. Hundreds of specific offences have been created, and the relevant law applied, since 1978. Procedural laws in particular have had to be amended to deal with **territorial** aspects of jurisdiction. Examples can be found in the case-law relating to the Criminal Code: Articles 113-5 (offences committed both in France and abroad) and 113-7 (nationality of the victim).

While the system of **time limits for prosecution** saw those limits extended by the law of 9 March 2004 from three months to one year for the most serious offences in this sphere committed via the Internet, the traditional rule that the time starts to run on the date of first publication is being maintained by case-law.

This right to be forgotten, however, is still a subject of debate, as shown by Google's recent offer (30 May 2014) to remove information from Internet pages following the CJEU judgment of 13 May 2014.

Means of investigation are also experiencing a very broad movement whereby cyber-weapons are being adopted and made subject to supervision, generally by the courts; without always achieving true equality of arms between those who enforce the law and those who break it, cyber-vigilantes, remote recording and digital infiltration are gradually becoming part of the legal arsenal to prevent the remedy from proving worse than the original evil.

4. Business

As **social networks** spread, **cloud computing** is used without limitation and **big data** make our heads spin, businesses can no longer just regulate themselves.

The question of laws' impact on organisations with changing structures and transnational chains of responsibility clearly arises, as the use made of video surveillance, geolocation and teleworking increases.

The ensuing proliferation of court decisions shows how difficult and necessary it is to avoid curtailing employers' and employees' rights and duties in the headlong rush towards a future made possible by unlimited technology.

The current focal points are assaults on electronic reputations – a subject on which there is a cruel lack of legislation, which should preferably be international – as well as data theft, business confidentiality and respect for privacy in a context of cyber-surveillance.

As the legislation currently stands, the courts can only consider the impact of new technologies in the context of long-established labour law, armed with the principles of proportionality and adversarial proceedings.

Infinite numbers of examples could be given, and their only merit is that they emphasise common challenges with a view to preventing the new technologies from being used as an excuse for restrictions or trivialisation of those human rights fully enshrined by over 200 years of struggles, even if they are not always honoured everywhere.

The success of reporting platforms, both public (such as PHAROS) and private (such as that of the AFA), shows that a feeling of resignation is the wrong reaction.

The on-line availability of good practice guides such as that of the CNIL and the growing numbers of Internet charters within the civil service and of staff with responsibility for the Internet within businesses are another positive sign.

The way ahead is indicated by the expected setting up of a digital court service and the adoption of strategic plans on personal data protection. The need for European instruments in this sphere to be updated is now clear to everyone. But the question as yet unanswered is that of whether it is the new technologies which give rise to new behaviours that new legislation is then needed to regulate, or whether new laws, could, more proactively, influence behaviours at the stage at which the new technologies are not yet fully available.

My own country learned a hard lesson when its wartime Maginot line, designed to keep it secure, proved unable to provide security on every front.

It is obviously essential to appeal to users' reason, but mere teaching has never deterred all possible excesses. In 1831, the *canuts* rebelled in Lyons by burning their looms, symbols of a new technology which they considered to represent too great a danger to their living standards. Nobody in 2014 is really considering doing away with the cyber-world, but experience has shown that the harmony of any society requires a striking of balances acceptable to the greatest numbers.

Within the area governed by European law, such a balance necessarily requires new rules and regulations, the dissemination of good practice, and an evaluation of the action taken by each state in a sphere where it is always unhealthy for existence to be too far ahead of essence.