COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 13 April 2015
cdpc/docs 2015/cdpc (2015) 5

CDPC (2015) 5

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

DRAFT REPORT ON THE IMPACT OF THE NEW TECHNOLOGIES ON BEHAVIOUR AND LEGISLATION IN THE CRIMINAL-LAW FIELD

Document prepared by Mr Yves Charpenel,
Senior Attorney-General at the Court of Cassation

CDPC website: www.coe.int/cdpc
CDPC e-mail: dgi-cdpc@coe.int

1 Introduction

Since the appearance of the Arpanet in 1965 and the Internet in the years that followed, the startling and universal proliferation of this new technology has had a sustained influence on our behaviour.

The extent of these changes has naturally had significant repercussions on the rule of law, whose very existence and purpose are to regulate human behaviour.

Three factors make the understanding of these changes difficult but essential.

First, the sophisticated technological dimension of these new tools which does not fit into our traditional legal culture causes legal professionals – those who make laws and those who apply them – to doubt their ability to fully come to terms with all the issues at stake.

The various prospective studies on information technology undertaken throughout the world tend to indicate that this evolution is not slowing down.

The emergence of cloud computing, for example, and of professional or private social networks continuously gives rise to behaviour and practices with which the existing social and legal responses struggle to keep pace.

Applying the traditional legal responses to these new situations is today no longer able to ensure that everyone has satisfactory access to the law and a sufficient degree of certainty with regard to the social, economic and political ground rules.

The second factor is the eagerness of users worldwide to acquire the products available on the market using these new technologies, most often without being aware of or giving any thought to the consequences on the rules of social life.

The importance of the new technologies market, linked to its universal proliferation and the success of global trade policies further adds to the dynamic developments taking place, in which the determination to charge ahead clearly prevails over any thought given to taking an objective view and assessing the consequences.

Lastly, the speed of technical developments and of their appearance on the market leaves no time to draw up and disseminate new legal norms and develop new legal practices.

At European level, for example, engaged for more than 60 years in a long process of pooling legal principles and rules, the new technologies create the reality or appearance of a unification of practices, extending moreover to the whole planet, with no framework having been laid down to monitor and control the risks inherent in these changes.

These asynchronous changes are to be seen in all areas of our lives, whether at home, at school, at work, in the courts, in the political arena, in the reform undertaken in the area of parental relationships, artistic creation.

While no aspect of our societies would appear to escape the effect of the new technologies, the inherent uncertainties are particularly in evidence in the criminal-law field.

This is the field which seeks to prevent and punish any violation of the social rules which are most important for a society at a given time, and it has been radically transformed and amplified by the dramatic increase in cybercrime.

In this extremely sensitive field of criminal activity, the Internet, more than any other modern technology, should prompt us to reconsider the fundamental issues justifying the existence and defence of the rule of law.

When more than 35% of the world population uses the Internet, it is not surprising that the new rules which little by little will be applied to these users, must be assessed and compared with those – set out in the legislation in force – designed to apply to the entire population.

Between hopes and risks, trust and resignation, it is imperative that the rule of law should provide responses to the triumph of the new technologies, for if not we will see emerge the figure of the machine (and of those who create it) as the compass of a society losing its bearings, a society lacking in values and one in which the law is foundering.

The darker flip-side of a society in the process of widespread digitisation is the emergence of unashamed cybercrime jeopardising the values of our democracies.

These democracies have begun thinking about these questions and taking action, in the difficult task of seeking to reconcile effectiveness and respect for the fundamental principles of criminal law.

This question is particularly strategic in the European area which has different co-existing criminal-law systems for which attempts are being made to bring about harmonisation.

Until we have completed the complex process of harmonising European criminal-law systems, with all the possible variants between continental “hard” law based on written law, and the “soft” law of the Common law countries, based more on a pragmatic examination of case-law, there is the very real danger of our now being faced with a “fluid” law which disconcerts more than it reassures.

In an attempt to identify as accurately as possible the situation of the criminal-law field grappling with the digital revolution, we should bear in mind the importance of the principle of consistency, suggesting a response which will avoid a fragmentation of approaches, the principle of compatibility, ensuring the continuing development of the rule of law in line with the principles established by the European institutions, and the principle of effectiveness, without which both the predictable and unexpected impacts of the new technologies will remain outside the law.

There is an ever-growing number of public reports on the rise of cybercrime, as illustrated by, for example, the Europol report published in February 2014, the French report by Marc Robert, also published in February 2014 and the Swiss report, published in March 2014. The conclusions in these reports generally coincide with those of countless others by private companies, all of which state that the threat is spreading.

Of course, it would be wrong to regard the impact of these technologies on our behaviour and our laws as necessarily impenetrable; but it would also be wrong to imagine that we can bring them completely under control.

The aim of this report is to present a synoptic view of the main issues involved and the fault lines visible at the intersection between the criminal-law world and the expansion of the new technologies.

It seeks only to identify the parameters of a future set of rules, striking a balance between freedom and constraint, which it is absolutely essential if the rule of law as we know it in Europe is not to be further weakened.

Plan of the report

2. The specific issues of the impact of the new technologies in the criminal-law field

The possible conflict between the criminal law and the Internet is a constantly present threat given that the Internet is by definition conceived and used as the ultimate area of freedom and that the criminal courts are there to tirelessly uphold the existence of limits to this freedom. Of course, it is inconceivable to imagine a society regulated entirely by criminal law or by the law of the Internet.

As it is always the case, progress or regression in the rule of law are based on our ability to strike the relevant balance at a given time between freedom and constraint and between private and public interests.

Our modern societies, and in particular the countries of Europe, have since the very first appearance of the Internet attempted to give full and sole precedence to the criminal-law approach, aware that one of the most necessary binding elements of our communities, the social contract so dear to the Enlightenment, is based on respect for criminal law, determining our ability to live together in the same territory.

2.1 A problem of definition

The definition of cybercrime has to be standardised at European level in order to facilitate co-operation actions between member States and established as a Community priority by focusing specifically on the sectors of activity most concerned.

Providing a precise definition of the nature of this priority is a concern shared by all the authors of the public and private reports that have been published successively over the last ten years or more.

Adhering to the general conception making cybercrime a polymorphous and evolving phenomenon grouping together all offences liable to be committed or facilitated by the use of digital technologies may be beneficial on two counts:

First, it covers huge flexible typologies including offences directly linked to information systems and networks, and more traditional offences, facilitated by using those technologies;

Second, it is a means of differentiating between behaviour that may be classified as criminal, i.e. defined by the law as a criminal offence and all the other – civil, social or commercial – impacts which do not directly fall under criminal law, which punishes abuses and excesses only where such are stipulated as constituting offences.

The even more general definition of cybercrime proposed by the UN (“Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them”) must therefore make it possible to focus on all offences connected with digital technologies, primarily the Internet.

Since the entry into force of the Budapest Convention, there has been a need for the debate to focus less on the question of the definition of cybercrime, which must of necessity be flexible and general so that it can reasonably anticipate developments in technology and behaviour, than on strategies to combat it.

The diversity of situations created by these new technologies is matched by the variety of possible criminal-law responses.

It is also necessary to put into perspective the importance of defining the new technologies so as to guard against the risk of the discussions being reserved exclusively for high-technology specialists, whereas the main challenge is to protect all nationals in the very widespread daily use they make of these new tools.

In this context, in which it is essential to identify the issues at stake and the public priorities, it is imperative to apply the same reasoning when determining the criminal-law field concerned :
Above and beyond the erudite legal categories, measuring the impact on behaviour and criminal law must take into account both substantive and procedural criminal law together with the associated criminal-law policies.

An inventory of European criminal law in this regard shows that these concerns are broadly shared by all member states which, since the Budapest Convention and its additional protocol, have embarked upon an ongoing cycle of exchanges and standardisation.

The richness and variety of this work, all of which seeks to find a relevant balance between binding principles and flexible implementation, between security requirements and respect for freedoms, must doubtless be further put into perspective.

The first educational requirement for the European institutions is doubtless to draw up a series of texts seeking to harmonise national legislations by means of guidelines free of the complexities of state-of-the-art technologies which are perpetually merging.

We need to find responses, setting out with greater clarity the principles and their applications in the European judicial area, to the inevitable grey areas associated with “cloud computing”, “big data” and “open data” so much a feature of current trends in the new technologies.

Such an approach is all the more strategic given that the criminal-law field, in view of the principles enshrined in the European Convention on Human Rights cannot countenance in its ground rules any lack of precision or persistent ambiguities.

In this connection, the Council of Europe must draw up new additional protocols regarding the definition of cyber-offences and setting out the conditions for mutual assistance in this field.

In order to ensure the effectiveness of the immediate future of the rule of law in Europe, it is essential to evaluate the impact of the European regulations that have successively been issued in various sectors of transnational crime, such as the EU Directives of 8 June 2000 on e-commerce, of 2002 on private life, of 2006 on data storage and the “data breach” Regulation No. 611/2013.

The work carried out in this context by the dedicated Europol group (EC3) could serve as a basis for a real operational monitoring centre regarding criminal legislation on cybercrime.

A quick look at comparative law on cybercrime outside Europe shows the same profusion of regulations and the need for a synoptic look at the effectiveness of these rules before contemplating moving ahead with the process of global harmonisation which is still in its early stages.

If we take the examples of the USA and Canada, essentially federal countries, we find both a proliferation of specific laws and a dispersal of the departments specialising in the fight against cybercrime.

In contrast, the People's Republic of China, a centralised State, concentrates its substantive texts in its Criminal Code, which devotes three articles to cybercrime (to be compared, for example, with the 248 cyber offences established in France), and assigns responsibility for enforcement to the Ministry of Public Security.

However, all of them strive to identify the main typologies of cyber offences rather than to fulfil the impossible task of producing an inventory of all forms of cybercrime.

On the other hand, none of them presents an accurate overview of the impacts of cybercrime on the reality on the ground nor do they offer a specific framework for international co-operation.

The main incentive for broader reflection going beyond the European criminal-law sphere may doubtless be found in the repeated occurrence of court cases such as WikiLeaks or PRISM which illustrate the universality of criminal acts and the diverse nature of the criminal-law responses proposed.

2.2 The challenges of the Internet for the rule of law in Europe

Based on the work to monitor the Budapest Convention and the Octopus plan which seeks to adopt converging positions with regard to Internet broadcasting companies outside the European Union, the following observations can be made, illustrating the magnitude of the challenges to be addressed.

First of all, transnational crime is thriving and innovative, according to the findings of the UNODC, the OECD and the ILO, and has found in the cyber world a means of expanding its traditional profits and considerable new sources which are clearly a powerful driving force of criminal innovation potentially devastating for our economies.

The adoption of common guidelines is clearly the relevant way to address this challenge while seeking to avoid the trap of the clash of legal sovereignty characterising the criminal-law field.

The Council of Europe's Convention on Cybercrime is the only binding international instrument dealing with cybercrime and, as such, should remain the reference for future European initiatives seeking to secure the adoption of guidelines for all countries drafting exhaustive cybercrime legislation, and also a framework for international co-operation to combat cybercrime among the States Parties.

The convention is supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems and is monitored by the Cybercrime Convention Committee (T-CY).

The mechanism set up, comprising regular consultation of Parties in at least one annual meeting of the Convention Committee, should be able to develop into a global system of mutual assessment similar to what has been provided for in the field of, for example, corruption or trafficking in human beings in order to give new impetus to the harmonisation of principles and rules on procedure and co-operation.

The first challenge is therefore very likely to be to continue to strengthen the existing common tools before considering drawing up new binding structures.

The second stage should be an attempt to raise awareness among European criminal courts in order to develop little by little a case-law able to put forward more consistent responses.

In this connection, the compilation of a European database of cyber-decisions could help speed up awareness of the proposed responses to common principles.

Such a community of European legal experts is all the more important given that cybercrime is progressing in a context in which all operators broadly fall outside the application of European regulations and are, to say the least, reluctant to be subjected to them.

Mark Zuckerberg (January 2012): *"The internet is the most powerful tool we have for creating a more open and connected world. We can't let poorly thought out laws get in the way of the internet's development. Facebook opposes SOPA and PIPA, and we will continue to oppose any laws that will hurt the internet."* He went on, *"The world today needs political leaders who are pro-internet. We have been working with many of these folks for months on better alternatives to these current proposals. I encourage you to learn more about these issues and tell your congressmen that you want them to be pro-internet."*

2.3 A problem of chronology

In order to take on board more effectively the challenges facing Europe, thought needs to be given to the ability of the legislative and regulatory mechanisms to anticipate or keep pace with the various technological developments which bring about constant and sometimes lasting changes to behaviour.

The objective is to make a normative strategic choice between timeless general principles, more technical regulation of the new tools to come and merely adopting a reactive approach.

Recent years have shown a situation in which technology and behaviour develop more quickly than legislation in this field. While it is not unusual for a police officer to run less quickly than a thief, it is still necessary to ensure that the race is not regarded as lost in advance.

The obstacles are well known, between an evolving and dominant technology which merely accentuates the development of unpredictable and reactive behaviours, and the diversity of legislation applied in a no less uncertain manner.

The radical novelty of the impact on laws and on behaviour in the criminal-law field is illustrated by the emergence of two very disturbing phenomena for the application of criminal law.

First, the question of **territoriality**, on which the necessarily restrictive principles of the jurisdiction of criminal courts are based, now faces the challenge of a virtual universe where the criminals and their victims, who are very real, come together at any moment, and potentially for ever, throughout the cyber world, in other words everywhere, meaning that any of the judges practising in a country where the Internet is accessible has jurisdiction.

Today, cloud computing makes the traditional problems of settling conflicts of jurisdiction infinitely more complex.

The question of **digital identity** is no less problematic for criminal lawyers upholding the European criminal-law principles of criminal procedure, since the new technologies can cast reasonable doubt on the natural or legal person who has actually intended to commit an offence, except by blindly following the technical arbitrations relating to IP addresses and the various data protocols.

In the light of this chronic instability of criminal law in our democracies, exacerbated by a tendency to regularly call into question the laws that have been enacted, the criminal-law response should take account, particularly with regard to the new technologies, of the irresistible shift from hard law to soft law, with the risk of having to make with a “fluid law” in which the extent, speed and fluidity of the flow of information foils the traditional responses and their primary purpose which is to ensure the legal security of everyone.

The question of the compatibility between judicial time and digital time remains to be addressed, but should be borne in mind when assessing the arrangements put in place, making sure not to upset still further the relationship between the requirements of stability and freedom.

2.4 The three weak points of the criminal-law response

Proper consideration of the criminal-law responses to the vagaries of new technologies presupposes a thorough evaluation of the main fault lines which digital technologies can impose on our legal and judicial systems.

In any event, the latter must anticipate, keep pace with or correct any behaviour that is likely to be characterised as criminal.

It is clear that the impact of the new technologies helps put further into perspective the effectiveness of laws on social behaviour. The difficulty becomes even greater when one bears in mind, as one must, that the effectiveness of any mechanism is only as strong as its weakest link.

Consequently, any legal advance cannot claim, in the criminal-law field, to fulfil its role, unless it ensures that it does not underestimate any of the three requirements of every criminal-law system:

First, the need to engage in **prevention** of cybercrime, which cannot be neglected unless one is prepared to suffer increasing infringements. Such a prevention policy is complicated by the extent of the field in question, i.e. all the individual and collective behaviours using these technologies.

It is further complicated in that it must bring it home to as many people as possible among the public at large that the immense facilities available to them nonetheless comprise risks and therefore limits.

Lastly, such policies, which must be commensurate with the universality of the cyber world, need to be transnational or at least be part of an effort to harmonise national policies.

Second, **investigations** are one of the areas most heavily impacted by the new technologies, especially in terms of identifying criminal evidence.

The widespread dissemination of digital tools in society logically results in the widespread existence of evidence available in digital form.

The requirements specific to criminal-law matters – the integrity and reliability of evidence acceptable to a court for the purposes of establishing the guilt of a suspect – are all the greater insofar as the technical appreciation of such digital evidence is not yet part and parcel of the culture of investigators and judges.

In order to derive from the new technologies benefits that are at least comparable to those seized upon by criminals as soon as they appeared on the market, it is imperative for the law to be clear in terms of both defining the methods for gathering such evidence and authoritative, legal definition of that evidence.

Given that investigators are forbidden from rushing headlong into technology without any control, it is essential that the law should define with precision and certainty the type of digital evidence that is admissible.

While the principle of freedom of criminal evidence and the concept of a sufficient body of evidence make it possible to ensure that digital evidence remains sufficiently flexible to keep pace with technological advances in the future, it is nonetheless necessary to specify in law the rules for gathering evidence, based in particular on the work of the Council of Europe in its guide to gathering digital evidence.

Lastly, **punishment** is the logical culmination of the fight against cybercrime and the underlying principles quite naturally are intended to be applied in exactly the same way.

Nonetheless, the criminal-law field is one of the areas that is most related to the specific political, social and cultural features of each country, including within Europe.

In other words, the challenge of the impact of new technologies on the criminal-law field can be addressed only on the fairly ambitious condition that we do not underestimate the choice of punitive responses tailored to the extraterritoriality of the new technologies, requiring us, as we have seen, to take into account both the risk of ignoring the *non bis in idem* principle and the risk of encouraging what could be termed “court shopping” given the existence of veritable “digital crime havens”, devaluing the whole exemplary nature of the criminal-law response.

One must also take into account the fact that the penalties laid down, supposing that one has resolved the questions of jurisdiction, definition of the offence and whether the offence can be attributed to a given suspect, will have an impact on the misconduct in question.

As prison sentences are reserved for the most serious violations committed by natural persons and since fines make sense only if those who are fined actually pay them, it is essential to establish the relevant criminal-law measures such as closing down the site, de-listing, publication of convictions via the media and confiscating the tools with which the offence was committed.

Further thought must be given to the nature, meaning and scope of penalties for digital offences.

3. Varying impacts on key sectors

The Council of Europe should highlight the sectors of activity where the cybercrime threat is greatest in order to identify and illustrate the extent of the affected behaviour, assessing the inadequacy of existing regulatory responses, both in individual countries and at the level of the European institutions.

Four main sectors can be singled out as warranting priority vigilance in the light of the offences already observed and the level of effectiveness of the responses that have been applied.

It should be noted that the constant diversification of what is commercially available in this field paradoxically helps increase the potential for crime. This is reflected in the capacity of the new technologies to influence an ever greater variety of human behaviour and the ability of criminals to take advantage of the new tools on offer.

3.1 Violations of human rights

Defining a common doctrine and long-term principles is a particularly strategic approach in a field in which the criminal impact of the new technologies is doubtless the most universal, that of human rights.

These rights, which since the founding declaration of the rights of man and the citizen have been repeatedly reasserted by the various European institutions, are particularly affected by the widespread availability and use of tools enabling apparently limitless exchanges and storage of information.

While the advantages for the freedom of information are considerable, the abuses that have arisen are no less significant.

Generally speaking, governments have attempted to respond and lay down limits, but in most cases often piecemeal and have tended to be more reactive than proactive.

It is also in this sphere that the relevance of laws intended to regulate the new behaviours spawned by the new technologies is the most strategic on account of the scale and speed of the impact on social mores and criminal practices.

Three areas closely related to the personal rights of each individual citizen have for several years been the preferred field for successful crime to develop: violations of one's private life, violations of legitimate secrets and discrimination.

Private life, by definition, concerns each individual's right to privacy, which criminal law everywhere has made a value whose protection is essential to life in society.

As the deployment of the new technologies has become more and more widespread, the European institutions and the national judicial institutions have constantly enacted legislation stipulating respect for one's private life as the limit to freedom of movement and access to data.

The new technologies, on account of their ease of use, storage and communication, have focused attention on the concept of personal data.

The new potential of open data, reflecting a strong commitment to enabling broader access to an increasing volume of data, has had the side effect of increasing the possibilities of violation in this privileged area.

These violations have the particularity of being carried out by very different perpetrators either driven by the desire to harm specific victims personally, or motivated by the lure of illicit profits without personal risk.

In any event, the rules on storage and communication set out by successive EU Directives should be monitored more closely and an emphasis must once again be placed on the balance still needing to be struck and enforced between the technological potential of digital tools and the essential limits which must constantly be redefined.

One of the worrying impacts of the growing accessibility of personal data is the survival of **legitimate secrets**.

Certain secrets run counter to the universal aspiration for greater transparency where they protect interests which the law establishes as essential for the equilibrium of all democracies, such as medical confidentiality, banking secrecy, religious confidentiality, professional secrecy, business secrecy and secrecy in matters of national defence.

However, the fascination of our society for a lack of constraints, particularly in access to information of whatever sort, makes the successive ramparts erected by secrecy laws increasingly more vulnerable.

To this must be added the bewilderment of legal professionals faced with the mysteries of the new technologies, making them reluctant to apply legal reasoning designed for a non-digital world to techniques with which they are broadly unfamiliar.

How then can one be content to see legal Maginot lines constantly circumvented by the invading tide of digital data?

How can one fail to feel disorientated when year on year the digital world amasses more data than all the knowledge gathered hitherto since the beginning of history?

Is not the real question whether private life is soluble in “big data” and whether “Big Brother” already rules alone over the kingdom of the cloud?

The third area where the fluidity and sharing of personal data have become problematic is in the field of **discrimination**.

This form of crime was identified as early as the additional protocol to the Budapest Convention as a key issue for the use of new technologies.

There were and still are huge areas that are concerned and today there are countless actual or potential victims: hate speech, sexism and racism, the prosecution of which is by and large unable to stem the flow.

The first results on Internet alert platforms show the extent to which our instinct was spot on as the number of discriminatory postings is constantly expanding.

The European institutions must do more here to ensure actual compliance with the numerous laws directly inspired by the principles of the European Convention on Human Rights. We need, for example, to make the existing prevention, detection and enforcement tools more widely available and step up the dialogue with States, associations engaged in the fight against all forms of discrimination, and Internet companies to reduce the regulatory contradictions in this field and foster more effective co-operation.

In short, we cannot simply be resigned to the many human rights violations inherent in the uncontrolled use of the Internet – and especially when it comes to the “dark net” where deregulation is now the rule.

While it has been possible to come up with a number of uncomplicated observations, their consequences have become more complex and must, more than ever, be addressed as part of a global anti-discrimination strategy.

A review of the case-law and norms drafted since the adoption of the Budapest Convention reveals the recurrence of a number of issues, all of which are topics which ideally should be studied and discussed in the future:

- is a legal status of digital identity feasible?
- how can one combine protection of privacy and instilling a greater sense of responsibility among users?
- the unavoidability of an Internet connection
- permanent traceability
- the trap of personal profiles
- the uncertain control over data put online
- the inadequacy of traditional responses to infringements of privacy
- the right balance to be struck between protection of privacy and public order requirements

As we can see, the new technologies have already marked a profound change in the definition of the right to privacy.

The role of the law is to stipulate the extent to which the right to know must prevail over the right to be forgotten.

The debatable legitimacy of secrecy and confidentiality shows how important it is for our democracies to address the difficult question of striking a balance between freedom of expression and protection of privacy.

In this connection, monitoring of Recommendation (2012) 3 of the Committee of Ministers of the Council of Europe which deals with freedom of expression with regard to global search engines could be enhanced by the parallels to be drawn with the reform currently in progress in the USA on neutrality of the Internet in connection with a draft Internet regulation proposed by the Federal Communications Commissions to foster “Net neutrality”, although it is not yet possible to guess whether it is Internet users or access providers who will benefit the most.

“Privacy may be an anomaly”, Vinton Cerf, Internet futurist at Google

3.2 Organised crime

If we look only at the most recent studies, such as the White Paper on Transnational Organised Crime, published in October 2014 by the CDPC, the threat posed by the 3,600 criminal groups recorded becomes all the more serious and grows all the more quickly as use of cyber-tools becomes standard practice within these organisations.

Developments in digital data of all kinds and the ease of access and compilation of data afforded by the recent emergence of open data and big data have not gone unnoticed to criminals who see this as offering them greater latitude in carrying out their illegal activities, identifying vulnerable sectors and laundering their profits, with a personal risk of being prosecuted much lower than that incurred in “traditional” criminal activities.

The typologies recently proposed by Europol highlight the importance of having a thorough understanding of the diversity of attacks and attackers, identifying where the main security weaknesses are to be found and ensuring collection and processing that complies with the requirements of European criminal law.

Two of the most frequently encountered constraints in these investigations are the difficulty in overcoming the anonymisation of flows and the increasing porosity of social networks, the wrongful exploitation of which has become an ideal Trojan horse for cybercriminals.

There are four sectors in which these protean criminal groups are particularly prevalent and which therefore require specific counter-measures:

First, the growing field of **payment fraud,** whose origin and mechanism are primarily linked to recovering, selling on or manipulating bank data.

The impact of these illicit methods, which are generally carried out without the knowledge of their victims, is multiplied by the now widespread use of payment by bank cards, the success of e-commerce and electronic storage devices.

The international nature of the field of activity of organised crime lends itself perfectly to the capture and instantaneous recycling of financial data, seriously complicating flow traceability and the identification of the perpetrators, especially when the countries and institutions concerned have not set up a prevention mechanism to reduce security weaknesses and an operational national and transnational co-operation system.

The development of increasing overlaps between the criminal market and the legal market, bearing in mind the possible large-scale reinvestments of criminal profits in the economy cannot but prompt us to be watchful with regard to the temptation, cynically expressed by some, to incorporate criminal profits in the calculation of national wealth.

The creativity of criminal groups in this sphere, illustrated for example by the recent appearance of “ransmomeware” viruses, which extends on a large scale the art of financial blackmail, should prompt us to establish monitoring centres for new forms of digital fraud (such as the use of botnets) and make widely available updated typologies together with guides on how to prevent and combat them.

The **human trafficking** field is no doubt one of the most worrying, as illustrated by the studies carried out by several institutions such as the ILO which showed in 2014 that the market in human beings, whether for prostitution, forced labour or organ trafficking, produces annual profits in excess of €150 billion.

The UNODC, which considers this form of trafficking to be one of the most profitable along with trafficking in drugs, has shown the extent to which the use of new technologies has improved the traffickers’ profit prospects and security, in terms of identifying victims and putting them into contact with customers, organising exploitation and laundering the income.

These worrying trends, clearly identified in the GRETA evaluation reports, could be the subject of discussions and specific analyses in the coming months.

The example of **counterfeiting** is also typical of the criminal side of using primarily online sales sites making available to everyone, everywhere, counterfeit objects endangering not only the economy but also, increasingly, the health and safety of consumers given the wide-scale counterfeiting of medicines and spare parts.

This very flourishing market is no longer the preserve of a few individual “amateurs”, but is now managed as a veritable transnational criminal market with the self-interested help of distribution sites which derive benefit in terms of subscriptions or advertising.

It is therefore essential to gain a better grasp of the issues and realities of these large-scale violations of intellectual property rights, and to make headway in producing more effective rules governing the responsibility of Internet intermediaries.

Such new regulations are all the more urgent given that the majority of laws passed in this field focused mainly on penalising illegal downloading, which had a real but limited impact, leaving the field open to criminal groups on account of the lack of harmonisation of international rules.

Our democracies have also been quick to address the problem of **terrorism**, beginning to consider, as part of the criminal-law measures taken following 9/11 and the attacks in London and Madrid, exceptional procedures proportionate to the perceived threat.

Like those adopted to combat cyber-paedophilia, these measures include exceptions to the procedural limits on access to private data, imposing a precautionary principle and consequently a particular onus on Internet operators.

Neither the European institutions nor the member states can now underestimate the role that the Internet can play as a communication network for terrorists and as a means of propaganda.

Nor can they underestimate the risk of cyber-attacks or cyber-wars which pose a threat to their fundamental interests.

A commitment to combating modern terrorism more effectively inevitably raises the question of blocking sites. In practice this comes up against the extreme reactivity of Internet users and the possibility they have of using virtual private networks and taking advantage of the facilities offered by the dark net.

Nonetheless, evidence of the use by terrorist groups of social platforms to promote their activities opens up prospects for counter-measures, at least in terms of surveillance.

All these questions reveal a common point, which is the universalisation and the diversification of the activity of criminal groups, which cannot be effectively combated simply by the very uncertain hope of the future harmonisation of European and international legislation.

The answer, once again, needs to be found in establishing specialised investigative teams, an operational network of European law-enforcement agents and experts and highlighting the positive results obtained from drafting a guide of best practices in specific fields, building on the experiments currently being trialled in the Europol context.

3.3 The field of morals and leisure activities

It is not surprising that the new technologies have had a particular impact on the areas of human behaviour which are most characterised by a search for the greatest possible degree of freedom, in other words the field of morals and leisure activities.

The challenge is commensurate with a reality constantly fuelled by the record of court cases illustrating how easily legal boundaries can be crossed by ordinary citizens.

The difficulty for law-makers is all the greater in view of the fact that determining the boundary between the rights associated with fundamental freedoms and the unacceptable violation of those freedoms is a very sensitive issue.

Three examples can illustrate this manifest discrepancy between the law, nonetheless democratically imposed, and unlawful behaviour which needs to be prevented.

The first concerns illegal **downloads**, a practice that is particularly widespread in the European economic area, which despite that is very protective of rights associated with literary and artistic production.

The lessons that can be learned from the impact of criminal-law legislation in this field prompt us first of all to give consideration to long-term public awareness campaigns since the mere threat of penalties has so far had little effect on consumers who do not regard their action as being a criminal offence.

Second, we need to work out a global strategy vis-à-vis Internet operators and rights holders.

The second example concerns **on-line gambling** which, on account of the proliferation of individual players, is increasingly exposed to the appetite of organised crime already heavily involved in on-line sports betting which provides, via the net, access to unlicensed sites in an area in which national, EU and third-country legislation is extremely diverse.

The final example concerns "**cybersex**" where there has been a significant increase in sites offering sexual services for payment, and this profusion has helped turn the Internet into the new Eldorado of prostitution.

These three examples would raise only moral issues, which cannot be just a matter for criminal law, if they did not at the same time reveal, above and beyond a substantial modification of human behaviour, the emergence of genuine offences which cannot be ignored when they encroach upon fundamental values, such as the protection of minors, the prime targets of paedophiles and human traffickers.

All these examples once again show the importance of genuine education in use of the Internet, reiterating the shared values which could justify criminal law seeking to restrict the multiple freedoms offered by technology.

3.4 The business world

The business world is particularly impacted by the new technologies, whether it produces, manages or uses them, and at the same time is the target of multifaceted crime.

Particular attention must be focused on the new boundaries of economic crime if we are to have any chance of reducing the disastrous impact on our economies.

Whether computer crime specifically targeting the technological systems used by companies or common-law crimes bolstered by the new technologies, the threats we are facing today are considerable – these include illicit financial flows linked to prepaid payment cards, electronic or virtual currency (bitcoins for example), and high-frequency trading making effective controls inoperative.

Also linked to the increased use of digital technology in companies are attacks on IT assets and abuses relating to labour relations which raise the equally urgent questions of economic intelligence and employers' access to employees' personal data.

The vulnerability of the largely digital economy is doubtless the price to be paid for the productivity gains which the new technologies have made possible.

In order to avoid too uneven a playing field between cybercriminals free from any legal constraints and subject to too little an extent to the firmness of the law, and companies which are subject to the legitimate legal constraints inherent in the use of these technologies, our objective must be to identify more specifically the narrow path between deregulation which is incompatible with true rule of law and excessive (and probably ineffective) penalisation of certain economic processes.

4. Stakeholders affected to varying degrees

The diversity of situations in which an impact is felt and the fragmentation of normative responses should prompt states to identify all the stakeholders affected by cybercrime in order to seek synergies and provide justification for specific solutions.

The considerable differences of interest and position of such a diverse range of stakeholders make it all the more essential to take transnational initiatives aimed at setting up monitoring centres and expert groups to discuss possible connections in order to frame strategies which must, of necessity, be multidisciplinary.

4.1 The victims of crime

These are naturally the first to be affected. They are countless in number and have a varying level of awareness of the risks they face and of the steps they should take to protect themselves. They should be encouraged to get a clearer idea of the key ways to prevent, reduce or remedy their vulnerability to the criminal excesses associated with the new technologies.

In this connection, we need to promote policies to encourage the detection of these excesses and to help people take the decision to report an offence.

Much still remains to be done with regard to understanding the ill-considered behaviour of users of these communication technologies and the ways of raising significantly each person's level of vigilance.

Exchanges at European level must be stepped up to gain a clearer insight into how to strike a reasonable balance between the various and contradictory issues.

In addition, an inventory of possible partnerships with associations of users and public and private ethics bodies should help specify relevant and effective reparation in cases where penalties can be handed down for such offences.

4.2 The law enforcement agencies

These are on the front line to define and prosecute the criminal aspects in this field.

The adaptation of traditional law to the criminal excesses of the Internet, which was the first reaction of criminal law professionals, has shown its limits and has led to the development of new criminal law and new criminal procedure.

The scale of changes to legislation should not lead us to underestimate the extent of the changes in behaviour of these players faced with having to understand, define and identify this new form of crime.

Based on the efforts already undertaken, the measures to be taken vis-à-vis these particular players can be summarised in the following guidelines:

- continue with the harmonisation of criminal laws specific to the new technologies, in particular by ensuring that the European texts already adopted are transposed into domestic law;
- define a common framework of guiding principles on questions of jurisdiction and limitation periods;
- ensure the widespread adoption of aggravating circumstances in traditional crimes where use is made of these technologies;
- develop joint training and specialisation activities;
- set up a legal database of case-law in this field;
- assign specific powers to European criminal co-ordination bodies (Eurojust, Europol);
- encourage whistle-blowing systems and reporting procedures

4.3 Technology players and the criminal-law field

The development of the new technologies has had a considerable impact on public and private behaviours, but has also led to the emergence of new professions whose legal culture is not the most prominent feature.

Naturally, all these new categories of technology players are, however, subject to the rule of law, even though the latter may vary significantly depending on the country in which they were established or in which they are based.

They include:

- the **operators** who manage the communication networks,
- the **access providers** offering and routing information,
- the **hosting providers** holding and storing these data,
- the **content publishers** putting the data online,
- the **software publishers** enabling the data to be used,
- and bloggers, the specialist services in social networks and retail platform managers.

All of the above should be able to operate in accordance with harmonised rules, at least at European level, which set out their role, status and criminal liability regime.

This significant effort currently taking place is essential in view of the need for precision in criminal law, as illustrated by the current fluctuations in national or transnational case-law in this field.

The examples of the fight against terrorism or cyber-paedophilia show how useful it is to adopt a twin-track approach in which the operators are partners in the fight against the less serious forms of criminal misuse of the new technologies but, for the more serious forms, are required to filter suspect data or be required to file a declaration of suspicion in cases provided for by law.

Clearly then, there is a need to harmonise the law applicable to technical service providers and conclude co-operation agreements with non-EU providers, bearing in mind the fact that it is obviously of benefit for these negotiations, in which there is often an uneven balance in terms of the nationality and economic influence of the providers in question, to be conducted by the European states in a united and consistent manner.

The need to foster coherent partnerships between the public institutions and the main private operators can be seen everywhere as a prerequisite for any effective criminal-law response, i.e. one which is able to have a positive influence on illicit behaviours.

However, while the three main categories of players involved quite naturally have different views of the issues at stake, it is nonetheless possible to envisage responses that are consistent, based primarily on improved awareness-raising of the potential risks, the ability to detect real threats, the networking of skills to combat those threats and the choice of effective sanctions.

4.4. The perpetrators of offences

A fourth category of players – the **perpetrators of offences** – paradoxically can provide us with an example of the objectives to be assigned to criminal-law legislation in the field of the new technologies, bearing in mind the remarkable ability of traditional perpetrators to adapt to the new possibilities, and the emergence of new categories of perpetrators, well beyond the “hackers” or unscrupulous “geeks” for whom cybercrime initially seemed to be reserved.

Lastly, the feeling of impunity which is widely shared by these new criminals should prompt the supporters of the rule of law not to resign themselves to a punitive approach which is futile or ineffective in a field which is undoubtedly complex but in which the consequences are such that they warrant relentless efforts to combat the criminal activity in question.

We need only bear in mind that cybercrime is above all a crime in order to persuade ourselves to marshal all the efforts required to implement a genuine European criminal-law policy.

Clearly, such a policy cannot merely relate to the principles of criminal law alone, nor place responsibility exclusively on the technical operators.

Accordingly, we need to nurture a specific policy in its own right if we are to have any chance of bringing about a lasting impact on the increase in the number of cybercriminals, the diversification of the areas concerned and the rise in the number of victims affected.

5. The need to develop new responses

The challenge for Europe is to come up with a criminal-law response to the new technologies comprising a reduction of State powers while maintaining a minimum common body of law guaranteed by a competent judicial authority.

The choice of specific, appropriate and proportionate measures to take account of the uncertainty of the digital era presupposes an inventory of tried and tested responses and an incentive to apply across the board those good practices that have been acknowledged as effective.

There is no doubting the value of adaptable and negotiated measures in view of the dynamic nature of the technologies and behaviours concerned.

The experience gained since the implementation of the Budapest Convention presupposes a rethink of the role of the public stakeholders and proactive encouragement for public/private partnerships and co-operation between legal professionals and technology experts.

In terms of European strategy, if the rules of law are to be successfully adapted to address the risks of the criminal use of the new technologies, then the way ahead has to be to opt for a comprehensive approach.

Such an approach must be based on complementary ideas combining and strengthening awareness-raising of the public at large, prevention of the main risks, identification of offences, specialist investigation, the determination of criminal liability, the dissuasive prosecution of established facts and the establishment of ad hoc judicial co-operation networks.

Essentially, this refocusing could be based on existing institutions, instruments and experiences in the European area, the overall evaluation of which could constitute the first stage.

One of the positive examples that could be encouraged is the establishment by Europol of a J-CAT (joint cybercrime action taskforce) which fosters, in Europe and beyond, consultation, co-ordination and action more in line with the complexity of transnational cybercrimes.

Similarly, strengthening the role of European judicial assistance in enforcement matters could be broadly based on initiatives currently under way, first and foremost of which are those by the European crime bodies Europol and Eurojust in terms of gathering information and co-ordinating transnational investigations.

Both bodies have begun to tackle cybercrime, particularly in complex cases involving the new technologies.

Their commitment to acquiring mechanisms to protect their own personal data should serve as a model for all systems designed to “guard the guardian” to protect themselves against any abuse that could give rise either to excessive use of personal data or excessive transparency, dangerous for the security of investigations.

The key requirements which should guide future strategies are the following:

5.1 Legislating

The normative dimension is intrinsic to criminal matters but must involve both a review and updating of laws and a compilation of best practices.

This is the spirit in which the provisions of the Budapest Convention and subsequent European texts could be updated rather than rewriting substantive and procedural laws which would doubtless be out of step with the speed and unpredictability of digital technology.

Rather, it is on ongoing verification of the relevance of the principles laid down ten years ago that European legal efforts should focus in view of the future technological developments and the corresponding offences.

In procedural matters, the road map clearly points to placing the priority on making secure the digital weapons developed to combat cybercrime and to harmonising the rules on data interception, digital infiltration, data capture, the freezing of data, digital requisition and geolocation.

A summary of current European legislations, based on a questionnaire sent to member States, could prove a valuable source of information to help define more accurately the normative progress still to be made.

5.2 Understanding

The European and national monitoring centres, both public and private, should be encouraged and called upon to specify together the definitions and classifications of useful data.

This is so as to better exploit the capacities of the new technologies.

- The traceability of systems has been one of the critical points ever since the beginning of computing. Establishing this traceability has proved a dilemma for IT professionals and users, especially in connection with determining the technical constraints, processing time and storage and monitoring capacity.

- Other areas for attention include developments in search engines and their transmission speeds, such as the impact of the Cloud on storage capacity and the nature of the data transmitted, and the very principle of the Cloud.

This should help States have a better understanding of questions of traceability, which are fundamental for criminal investigations, and to benefit from the mass of available data which could constitute admissible evidence.

This could be done on a broad scale, provided that this evidence complies with the necessarily restrictive principles of all criminal procedures compatible with the principles guaranteed by the European Court of Human Rights.

As such, it is imperative to produce a compendium of admissible methods and practices so as to explain the processes involved in seeking evidence, whether structured, semi-structured or non-structured.

Mastering the new technologies presupposes international collaboration between judges, experts and police officers, so as to make available the relevant tools, such as surveillance and data capture.

These guides should be interactive and available online so as to ensure their scalability.

Clearly, it would be extremely helpful to have a **criminal-law expertise reference system** which should be widely disseminated to experts, investigators and judges; similarly, model appraisal mission forms would considerably help to harmonise and ensure the security of investigations throughout Europe.

5.3 Information

Prevention actions tailored to the various stakeholders should be applied on a wide scale, on the basis of national, European and international campaigns.

The specific role of the Council of Europe should be emphasised at various levels.

This could include disseminating the activities and methods that have proved highly successful, promoting study programmes in liaison with scientific universities to anticipate and clarify the technological advances from the point of view of the criminal risks, with humanities universities to study the associated behaviours evolutions and, of course, with

law universities to analyse the many impacts of the new technologies on substantive and procedural law.

The European institutions could, in addition, step up their support via specific programmes with the training institutions for national enforcement officers.

5.4 Enforcement

In order to develop an effective criminal response, there has to be progress made in the typical issues of the criminal dimension of the new technologies, such as the harmonisation of substantive laws and the conformity of procedural laws.

Rather than writing or rewriting rules on questions which continue to be heavily characterised by the principle of sovereignty, such as the question of territorial jurisdiction, efforts could focus on the compilation of a European catalogue of the penalties laid down and a file of the sentences actually delivered in connection with the national criminal records of the various countries.

It is also necessary to define a mode of communication for both technical operators and users on the existence and consistency of the sentences handed down.

5.5 Co-operation

Identification of the key partners is a prerequisite for any successful instance of international co-operation, particularly in the field of judicial assistance where mutual trust and the verification of common principles and procedures are essential.

The conditions for success are based on tried and tested principles in the member States.

They involve the setting up of dedicated professional networks, similar to the European judicial network, and common training which can, where appropriate and in relation to certain specific topics, be extended to other stakeholders, such as user associations, organisations representing professionals in the new technologies or university networks.

Co-operation should also combine a multilateral and a bilateral approach, bearing in mind in this particular field the risk for European law of dependence on non-EU technology.

To this end, there would be nothing but benefit in drawing on the activities of the Cybercrime Convention Committee, tasked with monitoring the Council of Europe's Convention on Cybercrime, and its role of updating the cybercrime threat.

It is also necessary to make an inventory of the initiatives taken by the international organisations and the private sector in the cybercrime field as soon as possible.

In short, the reasonable and appropriate measures that could be envisaged in the short term (following on from the already existing European instruments) for a more effective criminal-law response to the changes in behaviour brought about by the new technologies could centre on the following three main lines of approach.

The first is to raise more effectively the awareness of European users to the criminal risks of the new technologies and the best practices which can help reduce the extent of those risks, in particular by means of monitoring centres and reporting platforms.

The second is to ensure specialist training for European law-enforcement officers using shared knowledge tools and to set up infra-national, inter-European and international co-operation and exchange networks, placing an emphasis on public/private partnerships.

The third is to focus on mutual evaluation techniques in order to bring about changes to and harmonise practices and regulatory frameworks.

6. Conclusion

For more than 20 years our societies have welcomed the “digital revolution”, eagerly and unfailingly embracing the extraordinary prospects of progress for all of our behaviours.

As so often, “existence precedes essence” and it was only gradually that the limits and dangers of these new frontiers began to be perceived.

Criminal laws have also begun to play its role of monitoring, identifying and penalising the abuses that have come to light.

Now, the aim is to speed up the construction of a genuine European digital law-enforcement area and to make it an inhospitable place to cybercrime.

This presupposes acknowledging that the digital society has created new rights and duties and ensuring that our common European legal heritage continues to resolutely perform its role of reflection, anticipation and regulation.

“We become what we behold. We shape our tools and then our tools shape us.”
Marshall McLuhan, *Understanding Media, 1964*