Law facing information and communication technology (ICT)

Poullet, Yves

Published in:
Progress in science, progress in society

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Law Facing Information and Communication Technology (ICT)—Conflict or Alliance?

Yves Poullet

Abstract Internet definitely is everywhere in our life and even models our behaviours and relationships. How the law is approaching the Internet revolution and to what extent the traditional legal fundamentals, structure, concepts and actors are surviving to this revolution? In the other sense, we would like to stress out how the law might also help to frame the technological infrastructure and operation at the service of societal values and the development of human liberties.

Keywords Information and Communication Technology · ICT Law · Internet · Self-regulation · Human liberties · Legal concepts Technological normativity · Data protection

Aim of this contribution Since more than 30 years, as lawyer and philosopher, the relationships between Law and ICT have been for me the essential of my research's concern. If Technology was, 30 years ago, a simple 'well-identified' product in the hands of certain specialists at the service of companies or administration for bettering their activities, obviously it has become with the Internet an integral part of our daily life, being ubiquitous in our activities and modelling our behaviours and our relationships. In that context, if Law has been traditionally the way by which our societies are framing our societal life in all aspects, it might be interesting to see how ICT have challenged, even in a crucial way, our legal environment, concepts, structure and put at risks our human liberties, fundament of the legal order. This article is devoted to these questions which definitively are still open in that tremendously evolving environment and calls for a better dialogue between Law and Technology if we want to keep alive our democratic societies.

CRID Founder (1979) (Research Centre for Computer and Law), Member of the Royal Academy of Belgium.

Y. Poullet (✉)
University UNamur, Namur, Belgium
e-mail: yves.poullet@unamur.be

A. Tressaud (ed.), *Progress in Science, Progress in Society*,
https://doi.org/10.1007/978-3-319-69974-5_9

Table of content We start with an eye-bird overview of the evolution of the ICT context (Section "About the ICT Context"), before analysing the challenges faced by the Law both as regards its traditional fundaments like territory and supremacy of the legal order but also more challenging as regards the legal concepts deeply challenged by ICT (Section "The Law Put into Question by ICT Technologies"). The following chapter (Section "Creation and Application of the Law Facing ICT") is dedicated to the transformation of the legal normativity and a comparison between legal order and technological normativity. At the end (Section "Liberties Within the Internet World"), we propose some reflections about our liberties within an Internet world. To conclude, we propose certain ideas as regards a new approach of the relationships between Law and ICT.

About the ICT Context

A rapid chronology Certain dates and facts might be recalled. The Internet's birth is dated from the famous US military initiative: ARPANET, launched in 1967, only 50 years ago as a way to decentralise the information in case of a Russian military attack. The TCP/IP protocol has been proposed in 1973 by Vint CERF, as a way to ensure an international language permitting to all computers to enter into dialogue. Initially, the use of the Internet has been reserved to restrained circles, mostly universities' people, regulating themselves and dominated by the dogma of freedom (free exchange of ideas) but rapidly, with the creation of the WEB (BERNERS LEE and CAILLAU) in 1990, as a collection of pages in HTML format, mixing together pages, images and sounds and having an URL address, so being accessible through the HTTP protocol, we did assist to a progressive transformation of this fair to ideas into a commercial fair used by the companies in order to extend their market and the management of their activities. The globalisation of the Internet is now a fact: in 2014, a milliard of online sites and three milliards of Internet users. In 2025, one forecasts 100 milliards of IP addresses.

ICT's infinite capacities Our digital universe is growing and growing, from Giga, Tera, Peta, Zetta (10^23 octets) and tomorrow Yotta bytes: today, we evaluate it to 1200 milliards × milliards octets (44 zettabytes in 2020).[1] In that context, three Laws are evocated: Moore Law, as regards the multiplication by two each 18 months of the processing capacities; Nielsen Law, as regards the multiplication by two each 21 months of the transmission capacities and Kryder Law, as regards the multiplication by two each 13 months of the storage capacities. Definitively we are entered in the **Big Data** era.

[1]Report EMC-IDC Digital Universe, "Extracting value from Chaos", 2011. Already in 2010, E. Schmidt, Google CEO, asserted that we are producing each two days five exa-octets of information. At his opinion, it was more than the information produced between the first appearance of the human culture and 2003.

To this first phenomenon, we must add another movement: I mean the trend to **Nano technologies** going from ambient intelligence (the 'Internet of things' or 'Smart dust': 150 milliards of connected objects mainly with RFID technologies)[2] to the present discoveries of the bioengineering which create the possibilities to intervene in the repair and modification of our ADN. So the technologies are everywhere in our homes, pockets, glasses, stores, streets and definitively embedded in our bodies and genes, conducting more and more our behaviour and what we are becoming.

… a deep modification The combination of these two phenomenon (Big data and Nano) leads to three fundamental modifications in the use of data.

a. The first deals with the **data collected, stored and processed**: due to the reduction of the costs of their storage, processing and transmission, Big Data is now a common activities of a large number of companies and administrations around the world. The data collected, stored and processed are more and more diverse (location, surfing or consumers habits, …) coming from different sources and a lot of them appear as trivial data even if their unpredictable combination might reveal very personal and sensitive information.
b. Precisely, as regards now the **applications** now available or envisaged at short time, through the use of meta data (Tag number, IP number, location identification, cookies, …), the collecting companies or administration are able to connect the data collected through different sources and therefore to **profile** people in such a way to have a very precise image of each Internet user and to act a priori vis à vis them. Two other kinds of applications must also be underlined: **affective computing** it means the possibility for data responsible to induce from different data (e.g. facial movements) in real time the emotion or sensitivity of person and to decide an action against him or her and **Brain–Computer Interfaces** which might act directly on the action or capacities of the human (like to increase his or her memory or to supply a deficient human organism).[3]
c. **Cloud computing**,[4] as a new way of data and application storage, and its different facets might be considered as a revolution. Data and software applications are no more stored or lodged on my laptop or mobile device and, for most of the companies, on their IT infrastructure but somewhere in the clouds. This reality raises the question of my or their master-ship of the data I or they are generating or building up. Where are these data located and for which uses?
d. Finally, as regards the **actors**, one pinpoints, beyond the traditional dichotomist presentation between the data subjects, from one part, and the data responsible

[2]G. Riva, "*The psychology of Ambien Intelligence: Activity, Situation and Presence*", Ambient Intelligence, IOS Press, 2005.

[3]M. Nicolelis, "*Beyond Boundaries, The Neuroscience of connecting Brains with Machines and How it will change our Lives*", New York, Times Books, 2011.

[4]M. Dikaiakos and others, "*Cloud Computing: Distributing Internet for IT and Scientific Research*", IEE Internet Computing 13 (5), 2009.

from the other part, the increasing importance of both, from one side, the ICT producers whose technology (e.g. the Androïd software) renders possible these applications and, from the other side, the omnipresence of what we call the 'Gatekeepers', it means the companies whose activities are necessary to get access to the information and communication services available through the Internet like social networks, search engines, music platforms, etc. All these services must be considered today as 'essential services' within our modern Information Society. These 'essential services' are no more offered by public authorities but are monopolised by a few number of private companies, the so-called GAFAM (Google, Amazon, Facebook, Apple, Microsoft) which progressively through a strategy of merger and acquisitions are dominating the global flow of information. The Google example (Google Map, Androïd, Double click, YouTube, Google news, Google search engine, ...) might be quoted on that point. Their economic power goes beyond most of the States' power[5] and creates a big risk for our democracies.

The Law Put into Question by ICT Technologies

The multiple challenges It is obvious that the Internet is dismantling the main fundaments of the law. The Internet is without borders and shakes even erase considerably the territorial limits of our States and thus the basis of their sovereignty (A) Traditionally, the unique source of the regulation is coming from the States or by delegation from International Public organisations like EU, UN and its subsidiaries (WTO, ITU, WIPO). With the Internet development, new private organisations have been set up and the concept of self-regulation has been considerably entered into force instead of that unique source (B) More important, certain fundamental legal concepts have been either revised, either deeply reinterpreted in such a way that they have loosen their initial meaning in order to consecrate new interests (C) Fourth, the legal actors are facing in their activities new challenges which raise questions about the principles of their action and competences (D) Finally, we pinpoint that ICT technology, through its 'ubiquitarian' characteristics and its indefinite capacities of control, puts into danger our liberties and freedoms, fundament of our democratic societies even if, in the same time, ICT technology enlarges them, as we will see it (infra).

[5]In that perspective we might understand the recent announcement of the Danish Government to open a Embassy for Google in Denmark, putting therefore on a same footing a private company and a State. Already in 1995, the NORA MINC Report to the French government underlined that IBM's economic power was equivalent to the French Republic.

The Disappearance of the States' Boundaries

Territory and Sovereignty It is common sense to assert that the Internet more and more ignores the national frontiers. The borders' control are no more operated within the territory of the State of destination but through the use of databases operated directly in the country of origin (see for instance the PNR system). The domestic flows of information are crossing different States (40% of the intra-European flows are circulating on the US telecom infrastructure) might be captured by foreign States through satellites or other techniques of wiretapping (see the recent Merkel's case and the famous ECHELON case revealed in 2000), which permit to US, UK, Australia to spy the communications exchanges throughout the world). 10 of the thirteen Internet root servers are located in the US. In all these points, the US predominance might be pinpointed even if EU authorities have tried to challenge that predominance by multiplying legislative initiatives and by creating an EU legal environment for the Internet and to impose the EU solutions. So the Regulation on applicable law to Contractual obligations (called Rome I, 2008) has imposed the concept of 'overriding mandatory rules' which refer to national rules which are deemed so crucial for the protection of a national political, social or economic order that they must be applied as a matter of course. The General data Protection Directive (2016) has clearly extended the application of the EU legal order to controllers not established in the EU when they are offering goods or services to data subjects established in the EU or monitors their behaviour. Recently, the EU Court of Justice (2015) in the SCHREMS case has challenged the EU Safe Harbour decision which authorised the trans-border data flows between EU and US companies for not complying with the constitutional requirement of the EU since US permits, to a too large extent, wiretapping and surveillance by US public Intelligence services. Other countries like China but also Arab countries have decided to have their own national Intranet network connected to the Global Internet network by a gateway in order to forbid any not controlled intrusion from outside.

The Internet Regulation Beyond the Traditional Legal Order

Technical standardisation and private organisations The principle of the State as a unique or at least main source of national applicable regulation and the International treaties conclude within Public international organisations as the main source of the international mode of governance has always been considered as a dogma by lawyers in our democratic countries. The Internet is deeply challenging that principle. The 1993 Gore's (US vice president) for a self-regulation of the Internet, it means a regulation by the private actors themselves was the point of departure of this movement justified not only by the global, technical and evolutionary characteristics of the Internet but also by the will of the US government to keep a certain control on the Internet through these private bodies, instead of losing

any power in case of International public bodies' competence. The multiplication of private bodies without any constitutional status but regulating globally our information society, beyond their competence on the technical aspects and their societal impacts, is henceforth a fact. So ICANN, a Californian non-profit organisation but having signed a memorandum of understanding (MoU) with the US department of Commerce, has taken the leadership as regards the regulation of TCP/IP and web addresses including the disputes on these topics.[6] It has to be underlined that this private organisation has mandated the International Public organisation, the WIPO for proposing an 'Uniform Domain-Name Resolution Policy' (the UDRP), a strange revolution where a private organisation dictated its law to a public organisation. IETF and W3C are ensuring the technical standardisation of the infrastructure, terminals and the web applications through expert's meetings and, at the end of a procedure founded on what they call a 'row' consensus, their decisions: the famous not well called 'request for comments'. As said, these private bodies are regulating indirectly economic and societal aspects of our life, so for instance when the IETF has decided to define the technical norms permitting the existence and functions of the cookies or when W3C has developed the P3P system (infra).

Self-regulation—Towards a global and complete normative system Beyond that emergence of private global standardisation organisations, there are another trends. First, the global companies, like but not only the GAFAMs, are developing their own privacy policies, codes of conduct, terms of Agreement, all these mechanisms often conceived in their content independently of any reference to national legislation. Recently, Facebook, Twitter, Microsoft and YouTube have published on countering illegal hate speech online (May 31, 2016) and more recently, they developed together the Hash-sharing initiative, which provides a unique digital fingerprints identifying terrorist content and preventing any apparition of the content elsewhere.[7] Second, at a large scale we see flourishing codes of conduct, codes of deontology, labelling systems and alternative (alternative to the national public jurisdictions) online dispute resolution (ODR) mechanisms, which are offering more rapid and effective sanctions (like blacklist, loss of label, ...). To explain the ODR success, we pinpoint the globalisation of operations caused by the Internet and the relative inefficiency of international private Law to solve them. To conclude, we see, on the fringe of our traditional legal order, the increasing development of global and complete self-regulatory systems, since the adoption of normative rules, setting-up of controlling methods, ad hoc jurisdictions and proper sanctions.

From WSIS to the EU approach—Multi-stakeholders and/or co-regulatory approaches Against that trend to a global privatisation of the Internet regulation, international public authorities have reacted. The UN General Secretary launched in

[6]As regards the Internet of things, EPC (Electronic Product Code) Global (a joint venture between private bodies) is regulating the world of connected things, having created the Object Name service in parallel with the Domain Name service operated by the ICANN and defining different protocols for connecting and interconnecting the different objects and their producers.

[7]This code of conduct has been evaluated by the EU Commission at the end of 2016.

2003 (Geneva) the first World Summit of the Information Society (WSIS), followed in 2008 by another Summit at Tunis. The final 'Declaration of Principles' looks like a sort of Constitution of the Global Information Society. It asserts the fact that Internet is a '*global public resource*' and introduces the absolute need to set up a '*multi-stakeholder Governance*', it means '*the drafting and implementation by the States, the private sector and the Civil Society, each of them in the limits of their respective competences, of the norms, rules, procedures, decisions making and common programmes appropriate to the modelling of the evolution and usage of the Internet.*' Despite this clear assertion, we have to recognise that International Public authorities have not been successful in asserting their place. The fact that different organiations might be competent for the same problem might explain their weakness and the fact that they are acting in different ways. So as regards the regulation of the Intellectual Property, UNESCO, WIPO and WTO have not obviously the same point of view and contradictory approaches might be expressed by each of them. The tentative to set up a public Internet regulatory body has been clearly rejected by US authorities, only an Internet Governance forum, without any regulatory competence but simple discussion forum, 'guarantees' the survival of the 'multi-stakeholder' governance asserted by the WSIS.[8]

The attitude of the EU definitively vis-à-vis the Internet self-regulation has to be underlined. On different themes, EU clearly has pleaded for a coregulatory system, asserting the predominance of the public regulation without excluding the private regulation but fixing the limits of it. Co-regulation means the mechanism, whereby a legislative Act entrusts the attainment of the objectives fixed by this Act to parties (NGO, Consumers' representatives, Companies' associations).[9] So in different domains, like Data Protection Regulation (1995 and 2016), Freedom of expression, Electronic commerce (2000), Services in the Internet Market (2006), Copyright issues (in course of debates), Racism and xenophobia (2008 within 2016, the conclusion between EU Commission and Facebook, Microsoft, Twitter and YouTube of a code of conduct on countering illegal hate speech), the EU Directives or Regulation are referring to more specific provisions (codes of conduct, Codes of deontology) or mechanisms (labelling systems, certification or accreditation procedures, technical means) which are defined by the actors themselves. The EU claims for transparent and effective mechanisms of private regulation including all the concerned stakeholders. This approach seems to offer an added value to both pure self-regulatory and public regulatory system since it combines the fundamental legislative choices with a better effectiveness and evolution of the norms, in the hands of the private sectors after discussion with organisations representing other interests and under control of the public bodies.

[8]It must also be noted that ICANN has created the 'Governmental Advisory Committee' within its complex organization.

[9]That co-regulation system might be considered as a 'top down' approach, compared with a 'bottom up' co-regulatory approach where in a first step, private actors are defining themselves their self-regulation before in a second step to approach the legislators in order to enact and give a legal enforcement or accreditation to their practices.

The EU attitude followed by certain countries like Japan, Latin American countries, even to a certain extent Canada, represents another model than the US one. It leads to a difficult coexistence of these two models in certain areas like especially the domain of Privacy or Freedom of expression. As regards Privacy, the OECD self-regulatory Guidelines are promoting self-regulation in the same time when Council of Europe and EU are adopting the legislative approach.

Legal Concepts Facing the Internet Context

The legal order has been construed on different concepts which have been defined in a societal context quite different from today and were taking into account a certain equilibrium between different legitimate but contradictory interests in that context. Technology is radically affecting this context and might affect sometimes deeply the actors' powers in a positive or negative way. ICT is transforming our social relationships and the way the technology is interacting with us. Considering that new reality, the law has either to reconsider the concepts developed in the traditional world and to maintain the traditional equilibrium embedded within the legislation, either to give the traditional concept another significance or to create a new concept. I take an example: the concept of advertisement or publicity was defined as a communication to the public in order to promote the selling of a good or service. Today with the development of the one-to-one marketing and the possibility for website to deliver, without any additional costs, large quantity of information looking like objective information, it was needed [see the EU Directive on e-commerce (2000)] to propose a new concept, that of '*commercial communications' which is defined as 'any form of communication designed to promote directly or indirectly the goods, services or image of company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession* and to regulate it in an appropriate manner. In the Internet age, the extension of the 'press' notion has to be reviewed in a deeper way since anybody might through his or her blog or through other electronic means deliver a message and so influence the general opinion. This radical extension raises questions: to what extent the legal regulation including administrative and fiscal ones available for the traditional press actors and institutions have to be applied to these new actors? Can we consider Facebook or others social networks' operators as editors? The last example: the traditional concept of 'swindle' linked with a human behaviour aimed at deceiving another human being has to be rethought when the deceptive behaviour is committed vis-à-vis a technical device.

We might multiply the examples but in the following paragraphs, we would like to amplify a general principle. We do enunciate it as follows: the Law has to welcome the development represented by the technological innovation but according to what we call the principle of **technological neutrality** (see, infra, n° 13). This principle has a dual nature. It might be considered as positive since we have to see how through technological means the traditional functions and

equilibrium embedded in the traditional legal concepts might be ensured: therefore, we have to host the technological means according to the respect of these functions and equilibrium. At the contrary, the legal system has to fight against technological means which modify the balance of interests enshrined in legal regimes and concepts (infra, n° 13) or to accept the risk to create through the legislative procedure new concepts.

From the non-discrimination principle to the principle of functional equivalence: the Law of Evidence and of the Electronic Signature As regards the technological neutrality, the main idea is to prevent the Law from considering a barrier to technological development (non-discrimination principle). In the same time, it cannot be question of subtracting technological developments from the substantial requirements established by the traditional legislation but at the same time (positive aspect) it must be required that these developments are complying with them (functional equivalency): the state of technology has a legal and judicial value equal to the one conferred to the traditional state, provided that it demonstrates its capacity to realise the same functionalities as the traditional state. Two EU directives about, the first, electronic signatures and, the second, the electronic commerce illustrate these two sub-principles. So, the 1999 Directive on electronic signature enunciates: '*Member states shall ensure that an electronic signature is not denied legal effectiveness solely on the grounds that it is in electronic form...*' but requires for being recognised as equivalent to a handwritten signature, that guarantees of identification, authentication and not revocability are met. On a parallel way, the e-commerce directive requires the Member States to remove any legal obstacles which hamper the use of online contracts. This means that a contract cannot be deprived of legal validity on the ground that it has been made by electronic means. So the e-commerce Directive recognise as its duty the welcoming of technological developments that substitute traditional conclusion, the process of execution and archiving of contracts when these developments guarantee the respect of functional requirements, which originally justified the recognition of traditional processes.

ICT and Copyright The history of the copyright facing the ICT illustrates the importance of the dialogue between Law and Technology. How the legal concepts might be deformed in other to protect ICT products and services and how the technology might give to legal protection an extension beyond the equilibrium put into place by the legislator.

As regards the first assertion, the origin of the software protection by copyright might be recalled. It is quite clear, according to the specialists of copyright that this concept was not fit for a not artistic work, that the concept of originality might qualify only rare software and that the requirement about the access to the work and not only to the functioning of the work was not met. Notwithstanding these objections, the lobbies and finally the legislators have chosen to use the inappropriate concept of copyright in order to get the benefits of its universal legal protection.

As regards the second concern, the easy and not controllable plagiarism of works and images on the Internet and the difficulty to fight against illegal reproduction and dissemination has been denunciated as the 'Death of Copyright'. The use of technological means (Watermarking, Anti-copying software, Digital Rights Management Systems (DRMS), ...) did represent a technological answer to that risk. These devices enable the control of not only the initial access but also are fixing the conditions of the use of the work (restriction as regards the support or the duplication, the price and its payment). Others might detect automatically the plagiarism and denunciate it. The Law has been solicited to support these technologies in order to prevent their circumvention and recognise their legal value. Doing that, it must be recognised that the Law is going beyond the traditional limit of copyright. First, they might protect works which are not deign of copyrightability; second, in a lot of cases, these systems undermined the possibility of taking advantage of specific exceptions to the author's exploitation right which were precisely granted by the legislator in order to promote intellectual creation. Third, certain of these devices authorises to protect any part of the work even if so partial that they do not represent the essence of the work. Finally, we pinpoint the fact that they constitutes a sort of reversal of the *onus probandi*: traditionally, the proof of the existence of a copyright is at the charge of the person who pretends to the protection. The technical measures give to this person a sort of presumption, not easily rebuttable, that he (or she) benefits of the protection. To what extent, this alliance between technology and law is in conformity with the system of intellectual property designed to promote intellectual freedom and the plurality of expressions and ideas what impose to take into consideration the conditions of public access and the use of the intellectual goods. To define through technology a perfect control of the use of the intellectual creations does not respect that essential equilibrium at the core of the copyright regime. Definitively, at the contrary, with the movement of 'open document' or 'open access', based also on the recognition of the author's moral rights, technology might also be used as a way to disseminate these intellectual creation at the benefit of a maximum of users and in the same time to respect adequately the moral and if asked the patrimonial author's right.

Creation and Application of the Law Facing ICT

The legislative time schedule the evolution of technology leads to multiply the intervention of the regulators in order to face these continuous innovations and their impacts on the society. That leads to a shortening of the legislative process as regards their adoption but also their modifications. So it is frequent to see legislation adopted with a process of evaluation after 2 or 3 years ('sunset clause'), where yesterday the legislation was written for the eternity. It might be of interest to underline that more and more pubic authorities, especially international public organisations (notably, Council of Europe, WIPO, CNUDCI, European Union,

UNCITRAL...), are intervening no more through hard law it means legislation but through soft law it means more supple methods not requiring the long legislative process and in certain cases issued by group of experts like recommendations, resolutions, decisions. These new methods of regulation rapidly adopted are effective since judges might more and more inclined to afford to that soft law a real effectiveness. The last point, sometimes large delegations are given to independent administrative authorities in charge of the interpretation and often of application of the law. We might quote that phenomenon in audio–visual, media and telecommunication sectors and in domains, like data protection or freedom of expression.

The use of ICT in the application of the Law Different remarks might be addressed on this point? ICT have not only invaded our Courts and tribunals but also the offices of the auxiliaries of the Justice like solicitors' offices. They facilitate the constitution of files, their transmission and the notification of the judgment and their archiving in databases easily exploitable. That phenomenon has a great impact on the way the lawyers are working. So we see new practices developed by solicitors as regards the way they are communicating between us and with their clients and the Courts and Tribunals, obliging to modify the ancestral rules and deontology as regards their conduct. Their conclusions are more and more exploiting large databases and give more importance to the case law and to the comparative law than before.

Artificial intelligence is supporting more and more their opinions, identifying according to the facts and the psychology of the judges, the good case law, the appropriate arguments and the interpretation to be given to the legal provisions with the risks to have more and more a sort of normalised case law. The fact that not all the lawyers might have access to these information services and facilities creates another risk: the risk of discrimination between lawyers and therefore between citizens in their legal defence.

The phenomenon of ADR and ODR the point has already been stressed (supra). If the phenomenon has started within the US, EU has followed the same trend to encourage the creation of EU ODR platforms to solve contractual disputes that stem from domestic or cross-border online purchases between consumers resident in EU and traders established in EU (B2C). A directive and a regulation have been issued in 2013 and enunciate rules to be followed by these entities. They provide the obligation for these platforms to offer services effective, transparent (all the details of the procedure must be published on the website), easily accessible, without the need of legal representatives and submitted to the control of a competent authority designated by the member states to monitor their functioning and development. Consumer and trader must agree on that way to solve the problem. The consumer submits his or her complaint by filling a complaint form through the ODR platform. However, nothing is said about the quality of the 'mediators' which are dealing the disputes and the obligation to provide a solution in conformity with the legislation available. Normally (except for complex questions), the solution must be provided within the 90 days of the reception of the complaint.

ICT and Law Enforcement Authorities at the service of public security and fight against illegal activities All our behaviours including our criminal activities are leaving electronic traces, it might be the simple possession in your pocket of a mobile which reveals your presence at a certain place, it might be a message stored in a computer or transmitted through a network, it might be a video-surveillance detecting your behaviour or movements. Numerous legislation are offering new possibilities for Law Enforcement Authorities to collect these data from their own initiative including by penetrating in the personal computers of suspected people but overall to collect data processed by information or communication services, including social networks operators. Moreover, they impose to these private companies the obligation to cooperate with them and to denunciate criminal infringements.

As regards that authorisation, we might regret that the concepts used in these legislations are often vague and that the list of criminal offences which might be subject to these cooperation's duty is extended constantly. Always about this searching methods, the procedure might be launched sometimes without the judicial control. Another problem to underline is the increasing use of big data services to detect potential suspected persons not only as regards terrorism but also as regards social or fiscal fraud. It means these often trivial data coming from different sources and combined through an unpredictable algorithm are not related logically with the pretended illegal activity. So the colour of your car, your moving, your surfing habits, your residence, etc. might from a statistical point of view reveals that you are belonging to potential raiders. That use leads to a reversal of the proof. Once again like with the use of DRMS (supra), the proof that you are honest will be on your shoulders.

Technological normativity versus legal normativity A lot of applications of technologies have a normative impact. This impact is not necessarily viewed as such by their users. I would like to take two examples. When an insurance company proposes to their customers to equip their vehicle with a sensor which automatically might record your infringements, you as a driver are committed to accept this automatic and at distance control of his or her car's driving. In exchange of an important reduction of your insurance's premium, you agree to be controlled each moment of your life. The insurance company is allowed to detect if your behaviour attested by the black box embedded in your car and connected directly with the information control system of the insurance company is conform to the circulation rules. In that context, it is quite clear that you are incited to obey to the legal prescriptions in a very efficient way. Another example, if you know that the network you use commonly is able to detect the use of certain words or sentences you will carefully avoid these terms. In these two examples, technology is used to force people to adopt consciously or not a behaviour conform to that expected by the society and operates as fixing a model making more effective the legal order—but also I will come back later thereon- in a not refutable way.

More generally, the opacity of the world surrounding you creates the feeling that you have to adopt the behaviour you estimate expected from you. That's what we call the 'anticipatory conformity', we mean the fact that, even without clear prescription about what you have to do, people are inclined to follow a certain line of conduct. In 1983, the German Constitutional Court declared illegal for insufficient transparency the Census Law adopted by the Parliament in the following terms: "*The possibility of inspection and of gaining influence have increased to hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public(or private) interests. Even in certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficiently certainty which information about himself in certain areas is known and cannot sufficiently estimate the knowledge of parties to whom communications may be possible,* ***he is crucially inhibited in his freedom to plan or to decide freely…This would not only impact his chances of development but would have also impact the common good because self-development is an elementary functional condition of a free democratic society based on its citizen's capacity to act and cooperate***.".

Finally, technology might also negatively prohibit certain behaviours or positively force people to adopt other ones. Normativity through technology deeply differs from legal normativity at least in our democratic countries in different ways. First, with the legal order, it is required that the legal texts will be published in due time in order to permit a certain forecast by the citizens who might anticipate the consequences of its non-respect. Second, technology offers apparently at least a perfect effectiveness of the norms, what is not the case with the legal order: all infringements are sanctioned positively or negatively (refusal of an advantage). Third, and this point is at my opinion the most important: as regards legal texts, their interpretation might always be disputed by people themselves before the Courts, that is what we call the 'recursivity' of the norm what means that the application of the legal texts are always subject to new interpretations at the light of the facts and by the judges taking into account the human beings' arguments. Since the technology operates automatically and following a logic not transparent, the possibility to go before the Courts and to invoke another interpretation of the applied norm will be difficult even impossible. As Lessig asserts, technology constitutes a source of norms often more powerful than the legal ones.

Liberties Within the Internet World

Our liberties at stake the Internet has tremendously modified the exercise of our liberties, both in a positive way but also in a negative one. What concerns the freedom of expression or of mobility and the privacy, we underline different facts which clearly demonstrate this positive impact of all the ICT applications. The global characteristics of the Internet and its open character mean a man 'without

borders', a man able to transcend the traditional social normativity: when I am surfing on the web or navigating on social networks, 'I feel free' since I am not identified a priori through my handicap, my job or my residence. Due to the interactivity of the web, I am able to act on my environment, to express my opinion, to refuse or at the contrary to share views, to select my 'friends' and the websites I want to get access. Moreover, ICT applications will increase my action, presence and capacities to master my environment, to use robots in order to facilitate my daily life, able through telemetry to control at distance my home, my children, to find my way within an unknown city. Tomorrow with brain–computer interfaces or telemetric at distance system, I will be able to be an 'increased' man more clever, more armed against health diseases or genetic problems. Perhaps, after tomorrow, I will be multiplied, having at disposal clones of myself.

In the same time, we have to confess that technology might affect quite deeply our liberties. More and more, we are tracked in our moving and choices, we are under surveillance without always being conscious of it and unable to know why and who is putting us under surveillance. Big data and the technologies of profiling already described are collecting more and more data about us and reducing us to our profile. That leads to a man more and more manipulated: as asserted by the Google CEO: "*it will become very difficult for people to see or consume something that has not in some sense been tailored for them.*". In the end, as the German Court noticed, the opaque ICT system surrounding us and its incredible capacities to collect, store without limits of time and to process all the data generated by my actions to control and manipulate us lead to a man more and more normalised.

New issues and the need to redefine the Privacy concept To summarise, these technical advances, even if from a certain point of view they are increasing our liberties, at the same time are creating huge risks for them and are raising fundamental questions other than the traditional ones concerning the protection of our intimacy. So new issues, more salient and crucial, are now entering the discussion like the question of justice as regards access to these technologies, the risk of a two-tier society, the question of democracy when we consider economic-technical, broadly non transparent, governmentality and the question of social justice in relation to the consequence of profiling applications rejecting a priori and without appeal certain categories of population. The question of dignity in the Kantian sense of the word is also to be raised since it is clear that, analysed through profiling techniques that use data collected from a large number of sources, the human definitively is not considered as an end as such but as a pure mean put at the service of marketing or security logic. 'Algorithmic governmentality'[10] operates without the possibility for the human beings, who are subject to it, to challenge the reasoning behind what is proposed as a truth, precluding any discussion, criticism or debate. How do we face these new challenges? Is privacy an adequate concept to

[10]According to the expression of Antoinette Rouvroy, "*The end(s) of a Critique: Data Behaviourism versus Due Process*", in Privacy, Due Process and the Computational Turn, the philosophy of Law meets the Philosophy of Technology, 2013, pp. 143–168.

answer to all these challenges and, if yes, with which meaning and how do we envisage the relationship between data protection and privacy, which are considered apparently as at least two separate human liberties by the EU Charter on fundamental rights (2000)?

Recently an author[11] suggests to better scrutinise the relationships between the Sen's or Nussbaum's theories of capabilities and privacy. Under Sen, capabilities encompass the conditions which enable the citizens to become '*fuller social persons, exercising their own volitions and to interact with—and influence- the world in which they live*'. The interest of bringing closer together the concepts of 'capabilities' and 'privacy' is twofold. First, it underlines the fact that the individual's mastery of his or her environment is not obvious and does not depend on his or her own volition but presupposes an active role of the State, which in a societal and economic context will enable this possibility of mastery. Arendt, as noted in the thesis, would have spoken about the possibility of an individual realising his or her 'virtuality', in other words to make valuable choices within an uncertain environment. It emphasises the fact that privacy is not a liberty among others but does constitute the conditions of these autonomic capabilities and is thus an instrument for the flourishing of our human fundamental rights and freedoms. The right to self-development within a given societal context is an adequate criterion to define the outlines of privacy requirements, considered as a tool for '*sustaining the uniquely human capacity for individual reflexive self-determination and for collective deliberative decision making regarding the rules of social cooperation*'. The author insists on the fact that the concept of privacy is evolving in its concrete meaning since it will refer to different means according to the evolution of the socio-economic, technological and cultural context wherein that human capacity will have to develop itself. If privacy could be limited to the protection of home, correspondence and sensitive data in 1950, the new technologies, the globalisation of our economy, the profiling activities,… oblige us to give to privacy another dimension and to recognise new subjective rights in order to achieve our capacity for self-determination.

Data Protection at the Big Data Age Data protection legislation appears in that perspective as a historical answer to the risks created for our self-development by an information society and thus is directly derived from the privacy concept. Legislation creates procedural guarantees (duty to inform, obligation to register and so on) and subjective rights (right to object, right to access,…) in order to leave '*space for individuals to choose the lives they have reason to value*'. Ambient intelligence and the profiling activities authorised by modern technologies oblige us to renew our legislation in different directions. The first one, definitively, is to draw our attention to the technology itself. Traditionally, Data Protection legislations consider only the relationship between data controllers and data subjects considered

[11]Luiz COSTA, *Virtuality and Capabilities in a world of Ambient Intelligence—New Challenges to Privacy and Data Protection*, Thesis, University of Namur, 2015, Law, Governance and Technology Series, 32, Springer, 2016.

as a liberal subject, the relationship submitted to the DPA (Data Protection Authorities) control. From now, we have to consider the technology itself insofar as the danger resides in the software algorithms, the infrastructure, the functioning of terminals. We have to take care of the potentialities of the technology, the design of the ICT systems, and the logic behind the algorithms. We have to consider that the individual consent as a way to legitimate data processing is no more appropriate since the data subject has no possibility to negotiate correctly as an isolated person. Collective consent and class action must be recognised. Moreover, with the author, we plead for a risk assessment of ICT technologies and for public debates about new applications and their societal impacts. The second point will be to underline the crucial role of the State which has to create this space for democratic discussion and to preserve the conditions of a public sphere where every citizen might, with confidence, express him or herself and develop his or her own personality.

Conclusions

Technology is the problem it might be also the solution the recent evolution shows that facing societal problems, technology might offer better than a legislation adequate solutions. It is quite usual to mention on that point the development by W3C, a private standardisation institution (see supra, n° 9) of the '*Platform for Privacy Preferences*' *(P3P)*, a tool that enables internet' users first to define his or her preferences as regards privacy but also sexual content, nudity or violence used by the websites, second, to exclude automatically any access to sites not respecting his or her preferences and third to engage, in that case, a dialogue with the website not fulfilling such preferences. This P3P is one of what we call *Privacy Enhancing Technological systems* (PETS). Besides PETS, different other technologies as already quoted are protecting the Intellectual Property (IPETS) certain are aimed to restrict access, others are preventing certain utilisations of the work (e.g. Digital Rights Management Systems (DRMS)), others are aimed to detect illegal use (e.g. watermarking). As regards consumer protection, certain Consumer Protection Enhancing Technologies are also developed. For instance, pop-up containing certain contractual provisions questionable from the perspective of the consumer protection might appear in order to request explicit agreement on them before to enter into the transaction. All these technologies might be supported even imposed by the legislation. So, for instance, the EU directive on Intellectual Property will forbid any circumvention of any DRMS and the EU Directive on e-commerce will impose the use of a symbol to distinguish clearly what might be called 'advertisement' from simple 'information'. To be short, technology assists law and its effectiveness, which itself in a sort of exchange of civilities, assists technology.

Recent legislations are going a bit further imposing the use of technology compliant with the legislative requirements. The example of the recent EU Global Data Protection Regulation (GDPR) adopted in 2016, by the EU Parliament is a

good model of this new trend. It enumerates new principles, like the 'Privacy by Design' principle which requires to embed into the technological and organisational design of the information systems used by data controllers the privacy requirements, like the 'Information Accountability' principle which obliges the data controller to develop mechanisms to ensure the respect and the control of the Privacy Policies they are issuing. We might also mention the 'data portability' principle that requires the possibility for the data subject to transfer without any technical constraints from a data controller to another one (e.g. if I want to leave my present social network to another one).

Towards an environmentalist approach Another trend as regards the relationships between Law and Technology, Technology is reshaping our society and the relations between people within this society, especially affecting their respective powers. ICT are surrounding and influencing all our activities and do constitute an essential element of our environment. That is why we are of opinion that certain principles derived from the environmental law have to be implemented within Internet Law. Therefore, we are of opinion that the States have new roles to play in that context. First, through independent agencies, they must first alert about these modifications and the risks incurred by certain citizens. Second, they have to set up a multi-stakeholders' dialogue in order to provide a 'Technology Assessment' in order not only to anticipate the developments of ICT innovations but also to follow the technological evolution, since these developments are often unpredictable (so cookies' technology has been developed by IETF (supra) just for preventing the consequences of the disconnection of the communication with the website without assuming all the invasions of Privacy the evolution of the Web applications have since permitted; other example: RFID technology was created only for logistic reasons) and to have public discussions about the risks but also the advantages of that technologies. Third, we want to recall the precautionary principle available in environmental law, which must be applied each time certain technologies are putting into question or at risks fundamental values of our societies.

In the same perspective, it is noticeable to see that GDPR is requiring a Privacy assessment, prior to a data processing when the processing '*is likely to result in a high risk for the rights and freedoms of individuals*', notably when they are undertaking profiling operations or before processing sensitive data on a large scale and in certain cases a prior consultation of the DPA.

The call for an inter-normative and interdisciplinary approach Facing the technology requires from the lawyers a double humility: the first one is to consider that the ICT regulation is no more ensured only by legal texts. As previously said ICT is also governed by technical standards by the market's forces and definitively by self-regulatory documents. Moreover, the effectiveness of legal solutions is ensured better through other normative systems than by the legal systems themselves. All these facts oblige the lawyers to be humble and to dialogue with these other normative systems. Enter into dialogue with the tenants of these other systems in order to create complementarities between these different regulatory systems is mandatory. Assuming that, we plead however for preserving the essential role of

the Law. First, it is quite clear that the Law is at the service of the investment's protection, the security of transaction (electronic signature or evidence) and of people (cybercrime). The Law has to take into account values like education, universal access and multicultural dimension of our world but above all, the liberties and the dignity of individuals are an absolute requirement as regards the development of our Information Societies not as an individualistic request but as a condition of our democracies.

As regards the second point, in order to provide the appropriate solutions, the lawyers must adopt a double **interdisciplinary** approach. First, most of the technological developments must be examined through different legal branches to be correctly regulated. To take an example, if you want to regulate DRMS, not only intellectual property problems have to be evoked but, beyond that, contractual issues, privacy questions, non-discrimination and other constitutional principles, competition rules, ... must be addressed and solved in an international perspective. Second, in order to understand not the technology in itself but the human dimension of its usages, definitively the lawyer has to understand not only the very nature of the technology but confront his or her analysis with sociological, ethical, communication's specialists' opinions. We clearly plead for multidisciplinary teams beyond the traditional disciplinary walls.

At the Internet Age, the tasks of us lawyers is thus essential: with the complicity of all stakeholders and taking fully into account the merits and benefits but also the risks linked with the development of ICT regulate our always evolving information society in such a way to leave to anybody throughout the world a space to choose the lives they have reason to value.