Vulnerable Person. Data Protection and Digital Society

ANTONELLO SORO[1]

Presentation to the Italian Parliament of the 2015 Annual Report of the Italian Data Protection Authority (IDPA). Rome, 23 June 2015

The Key Importance of Data Protection

Progress and innovation have brought about in-depth changes in the way we live, move around and shape our world. Proof is given not only by the manifest changes in communication systems, but also by the even more substantial changes impacting business relations – such as the development of a data-driven digital economy, which is modifying the geographic distribution of power worldwide.

There are companies whose growth has caused havoc in time-honored mechanisms of competition since they can lay hands on the whole gamut of knowledge that is generated day by day by seven billion people.

This has to do with the exponential growth of Big Data, fueled by the intensive use of increasingly sophisticated and accurate computing techniques. This has to do with the Internet of Things and its manifold applications – from domotics to wearable technologies – which provide everyday objects with digital identities.

But this has also to do with the "wired planet" – the new dimension of our lives, which are tracked down not only via the Web but also via geolocation, drones and smart devices that can even process emotional or

1. Mr. Soro is the chairman of the Italian Data Protection Authority (IDPA) since June 2012. Prior to his appointment, Mr. Soro was Mayor of the city of Nuoro and Member of the Regional Council of Sardinia. From 1996 to 2012 he served as an MP in the Italian Chamber of Deputies. During his parliamentary term, he was member of several key bodies and committees, including the External Affairs, Social Policies and European Policy Affairs Committees. He worked on important dossiers and contributed to the drafting of many bills including the one on ethics rules for journalistic activities to protect wiretap data and legislation to protect crime victims.

dynamic information in real time. In this all-pervasive network of ever-interacting and interconnected things, man does run the risk of being downsized to a medium that can be analyzed and monitored in terms of behavior, profiled to better target his choices, kept under surveillance to bring about increasingly invasive controls that encompass, ultimately, our own homes and physical bodies.

Everything revolves around the unbridled collection of data.

However, we are our data in a digital society: thus, a vulnerable data is the same as a vulnerable person. This should be the starting point in the search for new, more effective safeguards of our freedoms.

What is being analyzed, broken down and reprocessed is our identity – thanks to algorithms that can determine key decisions not only in economy, politics or finance, but increasingly in our daily lives as well.

From telemedicine to online polls; from e-justice to e-health; from video surveillance to social networks and live streaming applications such as Periscope, from online press to genetic analysis of crimes: there is no area of public or private life where the processing of personal data is not a prerequisite, which makes it necessary to have sound safeguards in place so as to prevent that data from being used ‘against us' by stripping us of our freedoms rather than facilitating their exercise.

This in-depth change in the very making of our daily lives raises questions and concerns; it highlights the conflicts due to the multifarious dimensions of real life and points to the sensitive issue of the man-machine relation – the unspoken fears that artificial intelligence may become autonomous from man coupled, on the other hand, with the temptation to entrust technologies with decision-making processes that should be up to humans.

The scenarios of digital society conjure up major challenges we must tackle without either giving in to powerlessness or harboring useless feelings of hostility. We should get away from the lure of technology-hostile approaches or the fear of innovation without giving up on countering possible distortions and looking for ways to regulate this process – generally speaking, without giving up on living responsibly.

Against this backdrop, data protection stands out not only as a right related to one's intimate sphere, but as an indispensable tool to reconcile

technical feasibility and legal acceptability, ethics and progress – as a precondition to exercise all other freedoms.

It should be observed that both the Italian Court of Cassation and the UNO clarified recently – interestingly, almost at the same time – that rights should be afforded the same protection both online and offline, whilst digital identity is no less ‘personal' than one's real identity.

The IDPA's work is being carried out in the context of these manifold changes.

Towards An Use of ICT by Public Administration That Is Mindful of the Value of Personal Data

The vulnerability of unsecured data produces disruptive effects on data integrity, accuracy, and availability.

There can be no data protection without security, and ensuring security is increasingly difficult: only consider the exponential growth of cyber-crime, of which we all are potentially victims – from identity thefts to violations of e-payment systems up to DOS attacks for extortion purposes.

The first challenge this Authority has to take up consists in fostering a systematic approach to the protection of data and infrastructures at both public and private level.

In the digitalized public administration, security is a key target in order to build citizens' trust and ensure efficiency and transparency.

The IDPA has stepped in to carry out controls and impose security measures for storage systems, data flows, and the interoperable databases that are shared by public administrative bodies, local authorities, social security and other agencies.

Several decisions were adopted, often following on-the-spot inspections, and they mirrored the fruitful collaboration with the individual bodies – which usually complied with our guidance.

A major effort was made by the IDPA to enhance security of the public system managing digital identities, which is expected to turn into a veritable critical infrastructure as its efficiency and reliability will be a precondition for citizens to fully trust the use of online services.

Setting up a modern, effective public taxation system cannot do without the creation of new databases and the implementation and interconnection of the existing ones.

Several opinions were rendered to financial bodies including – most recently – those calling for amendments to the tax return forms introduced by the Revenue Agency; this allowed devising technical arrangements to ensure secure, logged, targeted accesses to taxpayers' data.

The same applies to the health care sector. Some of the key areas of the IDPA's activity included the digital storage of medical records, online clinical examinations, health records and reports.

Whenever the mechanisms in place were found to be inadequate as part of the many fact-finding investigations we carried out, specific measures were taken to block or freeze the processing – as was the case with some leading public hospitals.

Technological innovations must go hand in hand with IT security systems that can ensure data authentication and traceability, selective accesses via unique credentials, encryption, alerting and auditing mechanisms: this is where the IDPA focused its attention, among other things, when assessing the many ambitious projects to modernize Italy.

This is also aimed at countering the new vulnerabilities of digital society – which actually come on top of old, no less awkward ones: I am thinking, for instance, of a HIV patient applying for fee exemptions at the health care unit where he or she is employed, or of the student that changed his or her sex and has to submit his or her university degree, or of the controversial issues related to anonymous childbirth.

Towards Truly Dynamic, Functional Data Protection

We are fully alert to our duty of making the principles of our Code effective by doing away with blotched information notices – whenever possible – and requiring solutions to be implemented that are reality-oriented. We consolidated a virtuous path of discussion with industry in order to lay down shared rules that would be amenable to implementation.

Rather than devising unwieldy solutions that make enforcement ultimately impossible, we have been looking for new approaches – like in

the case of cookies and mobile payment – that do not hamper user experience and require users to be active as well as informed stakeholders.

However, simplification must be accompanied by sound transparency policies.

We spare no effort in order to prevent consumer data from being exploited, whilst not underestimating market requirements: this was the case in the opinion rendered to the Ministry of Economy on the system set up to prevent identity thefts in consumer credit.

As for employer-employee relationships, the growing recourse to ICT in corporate management and the widespread use of geo-location and smart camera devices have blurred what was once the clear-cut boundary between one's private life and life at the workplace. The legislative decree that is being discussed by Parliament will hopefully include the changes enabled by innovation into a set of safeguards to prevent unjustified as well as intrusive controls in compliance with both the principles set out in the law empowering the government to pass such legislation and the constraints placed by European law.

Monitoring equipment and facilities in greater depth should not translate into the unjustified profiling of employees.

It is increasingly necessary to reconcile corporate efficiency requirements with the protection of rights. This was the rationale underlying all the decisions taken by the IDPA as part of several prior checking proceedings as well as in connection with the guidelines on biometrics.

In the private sector, we launched specific investigations to check compliance with the orders the IDPA had issued to banks some time ago so as to enhance the security of both IT systems and customers' data.

In fact, security is key in the new EU Regulation, which is approaching the final stage of discussion. The draft Regulation would appear to put much emphasis, among other things, on the adoption of security-by-design approaches *vis-à-vis* technologies; further, it fosters data protection impact assessments and risk-based approaches and commits new, important tasks to IDPAs such as with regard to a EU-wide certification system.

Data Protection: A Compass in Our Digital Future

The digital economy has led ultimately to the concentration of powers in the hands of technological platforms that are increasingly exclusive and influential at international level. Still, a new phase was opened up by the judgments handed down recently by the European Court of Justice.

In November 2014, the European Parliament approved a Resolution that called for a split between search engine functions and other services, whilst the Commission launched an infringement proceeding on allegations of Google's abuse of its dominant position.

These are important signals as they can put a real hold on the overwhelming power of platforms; however, Europe should not overlook its responsibilities, given its backwardness in building up a fully competitive digital market: this is actually the main reason for Europe's dependence on non-EU technologies.

Our Authority has been working for some time in order to do away with the informational asymmetry and opacity that feature in the activity of digital market giants.

The order issued *vis-à-vis* Google aims at making the Internet giant comply with the same rules as European companies have to abide by.

The verification protocol undersigned by Google – a first in Europe – envisages regular checks to be carried out at the company's headquarters in California (of which the first one took place last May) in order to monitor compliance with the order; at the same time, it is a means to carry on a constructive dialogue on issues that are kept as a rule strictly confidential by the US company.

A procedure for the appropriate exercise of the right to be forgotten has been established; it makes it necessary for search engines to act as counterparts of the IDPA in tackling complex issues that cannot be solved by relying exclusively on technology.

Over the past year, seventy-three percent of right to be forgotten requests were rejected in accordance with criteria and considerations the IDPA has usually endorsed when handling the complaints lodged following such rejections.

We have been opening up a path to show that data protection can truly become a key to keep abreast of the complexity of the digital world.

From this standpoint, let me recall our opinion on the National Statistical Plan, which envisages the possibility to use Big Data for the first time, or the public consultation we launched recently on the 'Internet of Things', or the international survey addressing the multifarious world of web apps – especially those targeted to children or monitoring our health.

We are steeped in the digital society and get to know ourselves, the world and the others increasingly through technology – but we are not equipped with the required antibodies.

This is why a new 'literacy' campaign is needed to foster active, informed behavior such as to enable us to handle our data with care. Accordingly, awareness-raising cannot but become one of the key tasks allotted to this Authority. All institutions are called upon to engage further in reducing and bridging the divide between the protection of citizens in the digital world and the long-cherished safeguards afforded to citizens in the physical world.

As was the case with the environmentalist culture, it is necessary to make people aware that every step taken in the information sphere (the info-sphere) must be taken responsibly; that each and every one of us can and must make the difference, today, in order to improve our future outlook and bring about the sustainable development of a networked planet. This is the challenge faced by States and this challenge requires a global response – sort of a Kyoto Protocol for data protection.

Privacy and Security: Harmony Rather Than Discord

The digital dimension is bound to become the arena of international conflicts. The Datagate has shown that emergency-driven legislation focusing on the blanket collection of bulk communication data is both untenable in a democratic perspective and basically ineffective - whilst it also impacts the right to privacy to an unacceptable extent and without any tangible benefits.

The Datagate case has led the US towards the European model in balancing freedom and security – which was summed up most aptly by the

German Constitutional Court when it said that ‘the Constitution rules out that freedom may be the price to be paid for absolute security.'

Still, whilst the US are leaning increasingly towards this model, Europe is in danger of losing her identity in the realization of its fragility. It is as if Europe were facing with dismay the growing asymmetry between law and the unrelenting evolution of technologies as coupled with the demand for security coming from the public. This was signaled recently by the bills passed in Spain and France, as well as by the legislative process of Italy's anti-terrorism decree.

Indeed, several provisions were added to the original bill – which had been the occasion for a hearing of the IDPA before both the Chamber of Deputies and Italy's Judicial Council (CSM) – in the course of its enactment process. We had emphasized that those provisions would undermine the balance between privacy and security, whilst they actually underestimated the implications of specific technologies – for instance, with regard to remote interception technologies; this would severely hamper any oversight on the legitimate acquisition of the relevant data.

Scrapping the latter provisions was quite sensible, as were the amendments made to other provisions such as those that enabled preventive interceptions for any type of online crime and envisaged a substantial increase of traffic data retention periods independently of the type of crime.

The latter provisions were clearly in conflict with the stance taken by the European Court of Justice in its data retention judgment, where the pivotal role played by the right to privacy *vis-à-vis* security was highlighted.

Such a pivotal role was re-affirmed subsequently by the ‘right to be forgotten' judgment in the *Google v. Costeja* case, where the business interests of search engines were at stake.

Both judgments were handed down at the same time the US Supreme Court extended the safeguards against any restrictions on personal freedom to cellphone searches – and in so doing, the US Court drew a more than symbolic parallelism between physical body and electronic body.

Strategic Intelligence and Mass Surveillance

The three judgments recalled above share the view that data protection is the main precondition for freedom in the digital age. Data protection is seen as the right to the ‘integrity of one's personality' – an indispensable requirement to prevent democracy from giving in to the totalitarian concept of a ‘glass man' and the Net from becoming a law-free area where indifference to rights is globalized in the place of freedom.

One should fight against the ever-returning temptation to consider civil liberties as a luxury one cannot afford when facing terrorist threats.

It is from the pivotal role played by *habeas data* in our democracies that Europe should start in countering terrorism and all types of fundamentalism without giving up on her own identity and nature.

To do so, one should reconsider the privacy-to-security relation also in terms of how effective mass surveillance actually is – given that it proved far less helpful also as an investigational tool than ‘conventional' (i.e., targeted and selective) surveillance. This was shown most clearly by the expert committee set up by President Obama.

The best way to defend our security is by protecting our data - including the infrastructures and systems those data are stored in – and preventing bulk data collection. This can limit the ‘attack area' for terrorism, which draws increasing force from the Net in shifting from cyber-espionage to the very factual violence of terrorist massacres.

Accordingly, effective terrorism prevention should select ‘sensitive' objectives sensibly as a function of the respective risk levels and turn data protection into a structural component of the fight against cyber-threats – which is what we highlighted also when heard by the Schengen Committee.

This is actually what we have said repeatedly, first and foremost with regard to intelligence (especially strategic intelligence) activities – whose scope of action is much broader and less ‘targeted' compared to conventional intelligence as pointed out by the Council of Europe, so that they are liable to turn into massive surveillance if they are not limited to truly ‘sensitive' objectives.

From this standpoint, special importance should be attached to the introduction of ad-hoc information procedures in cooperation with the Security Intelligence Department, which are meant to ensure that processing by intelligence agencies is fully compliant with the Data Protection Code. Reference can also be made in this connection to the opinions rendered this year on the security measures regulations adopted by such agencies.

However, similar risks of 'data overload' may result, albeit to a different degree, if especially invasive tools are relied upon in taking evidence – such as by way of wiretapping records or phone traffic data – unless suitable security measures are in place to prevent misuse or the case-specific preconditions set out in the Code of criminal procedure are fulfilled so as to limit the use of such tools, which are intended for specific rather than large-scale applications.

In fact, any personal data that is acquired with the help of the above investigational tools (but also with the help of DNA sampling, since the relevant profiles are to be pooled into the national database) must be also protected after being collected in order to prevent all types of misuse.

From this standpoint, let me stress how urgent it is to make sure that the measures ordered by IDPA especially with regard to the Ministry of the Interior and Public Prosecutor's Offices are implemented in order to achieve security of the data they process as part of their respective tasks.

This 'security offensive' *vis-à-vis* public and private entities where personal data are collected includes the decision by the IDPA to lay down specific measures to be implemented by Internet Exchange Points (IXP) managers following ad-hoc inspections; this is aimed at preventing the routing of data traffic to providers from becoming a 'safe haven' that is accordingly liable to all sorts of misuse – which would produce devastating effects given the facilities at issue.

Indeed, the (recent) experience in some EU countries shows that this type of misuse does happen also in a democratic system – see the data tapping case in Germany, at the Neutral Exchange Point in Frankfurt, 2015.

Towards Truly Democratic Transparency

Legislative decree No. 33 of 14 March 2013 contributed significantly to doing away with secrecy as the main tool to exercise power and it also brought about changes in the relationship between individuals and authorities – from one based on unchallenged authoritarianism and bureaucracy to one grounded in ‘controllable' equality of arms and participation.

Still, several criticalities were highlighted in the course of its implementation, which have to do basically with the one-size-fits-all disclosure requirements.

Indeed, those requirements apply in the same manner to markedly different situations and organizations and do not take due account of the corruption exposure risk of the individual entities, of their scope of activity and/or the public funds that are allocated to such entities and for whose management they are accountable.

Thus, those regulations introduce identical provisions for highly divergent situations and risk undermining the overall balance of the relevant legal framework. The effects they produce are largely unrelated to the objective that ultimately underlies this legislation, i.e. ‘enabling public oversight on the discharge of institutional tasks and the use of public resources' as per Section 1(1) of legislative decree No. 33/2013.

The – often significant – limitations on privacy resulting from the above disclosure requirements may prove to be unreasonable under certain circumstances so that they may have to be reconsidered.

In fact, transparency as a tool promoting participation, accountability and legitimacy must be protected against any distortive or ‘muddling' effects that are tangible risks if it turns into a boundless crave for disclosure.

There is a real danger that truly significant information gets hidden by useless scraps of information, so that the public oversight on the exercise of power and authority is hampered rather than facilitated.

The muddling effect is a somewhat implied risk in the approach adopted by the Italian lawmaker: unlike the US FOIA (Freedom of Information Act), the Italian legislation refers to undifferentiated dissemination on the Net as the sole mechanism to ensure disclosure.

Accordingly, one should reconsider not transparency per se, which is a fundamental benchmark of public administration, but the mechanisms to implement such transparency, partly following the model devised in the FOIA - which empowers anyone, on request, to access public records; further, one should re-define both the scope and the substance of disclosure requirements as a function of their being truly instrumental to public oversight on the exercise of power.

Not always is publication on the Net the best way to inform, ensure transparency and thus achieve a ‘democratic' process: this is so because there is the risk that the information may be altered, tampered with, de-contextualized and reused for different purposes so that the requirement to provide truthful information would be jeopardized along with any meaningful oversight – whilst the data would never be ‘forgotten' once it ceases to be useful.

These are the concerns we voiced to the Government also by way of an analysis conducted jointly with the ANAC (National Anti-Corruption Authority) in order to highlight possible avenues of reform.

Thus, the real challenge consists in ensuring democratic rather than demagogic transparency, which can be beneficial to citizens and does not jeopardize their personal sphere.

Online Judgments and Transparent Justice

The same synergy between privacy and transparency should be at work in connection with the online posting of judgments. Publishing highly valuable data on the web such as those that can be found in a judgment and the underlying principles is unquestionably more ‘democratic' as it can make available an important set of information potentially to all citizens.

However, this ease of access is both an extraordinary resource for individuals and institutions and – paradoxically – the greatest source of the risks arising from online publications, as they can be indexed, reproduced out of their context and tampered with. In short, this type of publication may in no way be equated to paper-based publication.

This is why we proposed that judgments – given the current legislative framework – should not be indexed by all-purpose search engines in order to reconcile publicity of judicial proceedings and their final outcomes with privacy of the individuals involved in such proceedings for whatever reason.

In doing so, we attempted to interpret legislation that had been enacted 12 years ago in a forward-looking perspective so as to take account of the 'constitutional' framework in Europe and the differences between paper-based and electronic publications.

This solution is actually similar to the one adopted by Parliament – partly following our suggestion – in connection with parliamentary records; it is aimed at reconciling personal dignity, publicity of proceedings and integrity of parliamentary records.

As well as de-indexing the full text of judgments, one could more reasonably foster the dissemination of the juridical knowledge contained in case-law by publicizing judgments to the greatest possible degree whilst blanking any names they contain.

Implementing this solution would appear to be all the more necessary in the face of the stepwise computerization of judicial proceedings we are witnessing. In this connection, the safeguards the IDPA has suggested to Governments over the years when giving opinions on several instruments regulating the use of IT in judicial proceedings have allowed setting the highest possible standards in balancing transparency and efficiency of justice, on the one hand, and the protection of personal data on the other hand.

Privacy, Press and Judicial Proceedings

Equal importance should be attached to the balancing of privacy and freedom of the press with a view to enhancing the quality of our democracies. This is an area where there was no dearth of issues to be tackled in the past year as well.

Reference can be made, in particular, to the clarification that journalists must behave fairly in discharging their tasks – especially by

refraining from subterfuge or tricks, and even more from impersonation (which was the case in a complaint lodged with IDPA).

This stance was shared by the judicial authority dealing with the appeal proceedings.

Indeed, investigative journalism does play a key role and should be fostered as an extraordinarily powerful driver of democracy; however, it may not rely on practices that are considered to be criminal offences per se for the sake of getting at confidential or secret information.

A similar call on accountability was made repeatedly with regard to trial journalism and the need for complying with the principle whereby only material information should be disclosed – a principle that has been often violated (even in breach of the rules on publication of investigative records set forth in the criminal procedure code) because long excerpts or the full version of such records have been disclosed including transcripts of examinations or interceptions. This was instrumental to appeasing public curiosity but did not mirror any real need for transparency *vis-à-vis* the given judicial proceedings.

And this has been detrimental, at times irreparably so, to third parties, perhaps children or victims of the offences: their lives have been exposed and posted on the Net, perhaps forever.

This is why we issued blocking of processing orders to prevent additional violations in specific cases related to trial journalism – so as to protect both innocent bystanders and suspects whose lives and relations had been probed into at great length without whatever links to evidentiary requirements.

We also drew the government's attention to the need for reconsidering the balance between investigational demands, freedom of the press and privacy in the face of the increasing mediatization of justice.

Indeed, the fact that one is involved in a judicial proceeding on whatever ground may not justify, per se, a pillorying exercise in which sensationalism is passed off as freedom of the press.

Thus, we call for Parliament and the government to take up this issue by reconciling fairness in seeking and imparting information with confidentiality of investigations and ensuring the due proportionality

between privacy and investigational tools – a principle that was recently reaffirmed by the EU Court of Justice as well.

Right to the Internet and Rights on the Internet

The Network was the focus of growing attention also by Parliament especially during the past year. We witnessed several initiatives aimed at setting forth basic safeguards for the dignity of individuals in the info-sphere: from the draft Declaration for the Rights on the Internet to the constitutional bills on access, from the legislation on "cyber-bullying" to enhanced safeguards for children.

The Net is a dimension of our lives where everyone's personality develops – to quote Article 2 of Italy's Constitution.

If this is the case, one can argue that the Net has turned into a legally protected asset deserving protection especially to prevent its subjection to market rules – that is, to avoid leaving the worldwide protection of fundamental rights to the 'private law' arising out of contractual terms.

Thus, today's challenge does not consist in introducing legal constraints into an area that would be capable to organize itself if it were left to individual discretionary decisions of an ethical nature: in fact, it consists in defending the freedom of this boundless public space determinedly.

Along with its extraordinary power to foster inclusive processes and democratic, pluralistic participation, the Web has also shown – in line with the duality that is typical of all technologies – that it can magnify discriminatory, violent or harassing activities and produce disruptive effects. These effects often impact the weakest or those that are regarded – and depicted – as different.

The gamut ranges from grooming to inducement to hatred; from rape – committed offline and then displayed online, which magnifies its detrimental effects – to the 'voluntary enslavement' of child prostitution up to cyber-bullying in all its versions.

In short, it is not only everyone's right to the Internet, but everyone's rights on the Internet that have to be guaranteed.

This applies in the first place to children: they are the main victims of misuse, because they are not equipped to understand to what extent they can expose their (innermost) lives to the world and what risks they are running in doing so.

Paradoxically, the Web is where children's fragility is most evident – caught as they are in the gap between a delusory feeling of autonomy and their law-abiding conscience, between the experience of freedom and the need to act responsibly.

The Web is also where children commit violations on other children under the assumption of remaining anonymous.

This is perhaps the most tragic feature in the violent use of the Web: that is, victim and offender share the same fragility and are unaware to the same extent of the very tangible and ‘real' impact produced by every single step they take in the digital world. The only antidote to this can come from the fully-informed exercise of one's right to the protection of personal data and from a new code of ethics for the digital society.

This is what our Authority is aiming at day after day so that the Net's extraordinary ‘generative power' is used to foster everybody's rights rather than to violate them.