# SENSITIVE DATA, PRIVACY AND RIGHT TO BE FORGOTTEN

By Federica Resta

## Focus

*Habeas Data*

In his essay on the "loss of privacy", Umberto Eco entrusts the "authorities supervising over our privacy" with the task not only of "protecting those who want to be protected, but also of protecting those who are no longer capable to protect themselves." – because the attacks on privacy end up getting us all used to its loss. At a time when one increasingly commits important pieces of their own selves to the Net, to companies one purchases products from, the public administration one is using the services of, in short, to third parties, one does run the danger of failing to grasp the meaning and value of blurring the view over one's own private life.

It is unquestionable that new technologies have freed us, in part, from the domination of space and time; however, they also risk subjecting us all to new types of slavery by making the information society a society keen on reporting, surveillance, profiling.

Given these risks, the only veritable safeguard consists in making an informed use of the right to the protection of one's own personal data. This right is enshrined in the Charter of Fundamental Rights of the EU as a separate right from the protection of private life – which is closer to the right to be let alone mentioned by Warren and Brandeis – because of its being a precondition for freely deciding how to expose oneself to the world; it is the hard core of personal identity also in its social projection and is accordingly a prerequisite for human dignity and the unfettered building up of one's own personality.

Thus, *habeas data* is the counterpart of *habeas corpus* as regards the electronic body and digital identity.

Still, in spite of the pivotal role played by this right in today's configuration of citizenship, it is increasingly violated as shown by the activities of the Italian data protection authority. This is especially the case with journalism, an area where striking the balance between privacy and freedom of expression is probably most difficult, in particular in a democratic system like ours that is focused on the individual – that is, in a system that is mindful not to allow limitations on personal rights that run counter their very essence, not even in order to protect collective or social interests, partly in line with Article 52(1) of the Charter of Fundamental Rights of the EU.

## *Information, Identity Dynamics and Right to Be Forgotten*

From this standpoint, legal journalism is especially daunting a sector because this is where the need to afford citizens the required information on facts that are, generally speaking, in the public interest - also to ensure transparency in the operation of justice – must be reconciled with privacy as well as with the presumption of innocence principle. Further, it must be reconciled with the right of a sentenced person to be socially rehabilitated and with the dignity of all the individuals that are involved, on whatever grounds, in a judicial proceeding; above all, one should refrain from pumping up certain phases of investigations when the accused is especially vulnerable, in particular if he or she is the subject of measures limiting personal freedom. It is no chance that the Code of Criminal Procedure bans the publication of images showing handcuffed individuals – the rationale being exactly the need to protect human dignity at a time when the individual is most vulnerable. This is why the Italian data protection authority (the "Garante") prohibited a TV show from further broadcasting pictures of accused persons inside their own homes – also by way of the so-called "close-ups" – at the

time they were being arrested (see decision of 18 May 2012 – web doc. No. 1900914).

Another difficult issue has to do with the need for ensuring that news are as up-to-date as possible, since doing otherwise might be ultimately prejudicial to the data subject's dignity - whose image would not match with reality. In this regard, domestic and international case-law (especially from the ECHR) has emphasized the need for reporting on the evolution of a story that, if not updated, might translate into the provision of inaccurate information. This is the approach followed by the Garante in requiring online publishers to update their articles and news so that the data subjects' right to respect for their identities – in their current dimension – can be reconciled with citizens' right to receive (and journalists' duty to impart) information that is accurate, reliable and complete.

A similar approach – i.e., the updating of obsolete information or the non-application of indexing mechanisms to such information – was actually implemented by both Houses of Parliament, partly upon the Garante's impulse, to address the disclosure of parliamentary proceedings and works where personal data was contained that had become meanwhile out of tune with factual developments. Both the Garante and judicial authorities have been faced with complaints lodged by citizens requesting, among other things, the non-application of indexing mechanisms in respect of parliamentary proceedings that mostly concerned investigational activities by Parliament and contained (mostly) legal journalism information they considered to be in breach of their dignity – since such information failed to take account of the favourable evolution of the respective cases. Apart from the issue of the special regime applying to the Houses of Parliament, which fall outside the scope of the Garante's powers, this case shows that posting, on the Net, documents that are public by definition – being parliamentary proceedings – does raise new criticalities that call for equally new solutions.

Special importance should be attached, in terms of their number and

impact, to the cases where prejudicial information (usually relating to the coverage of judicial proceedings) failed to be updated after being stored in the online archives of dailies – which is a veritable breach of the right to be forgotten, that is the right to a thorough, topical representation of one's own identity that should mirror both its evolution and its dynamics. From this standpoint, reference should be made to the decisions taken by the Italian Garante vis-à-vis several online media in order to have news updated with regard, for instance, to charges or convictions concerning individuals that had been subsequently acquitted; in some cases, the Garante managed to prevent the autocomplete function of some search engines from operating in a way that was in breach of data subjects' dignity. Indeed, if the name of a person acquitted of a charge is paired automatically in Google's search field with words like "mafioso", the representation of that person on the Net as based on the search results cannot but be misleading. This is why it is so important for the information posted and disseminated on the Net to be continuously updated and made accurate – in order to ensure that the information is thorough and truthful and that the data subjects' dignity and identity are respected.

This is ultimately aimed at preventing the complexity of a person's life and image from being crystallized and downsized to a single detail – perhaps of minor importance or, worse still, such as to disrupt the meaning and rationale of that person's whole life (see, in this connection, L. Manconi, *Vita e dettaglio*, Il Foglio, 1.8.2012, p. 2; G. Amato, *Quei dubbi insensati offendono la verità*, Corriere della Sera, 29.7.2012, p. 11).

Thus, the right to be forgotten is supplementary to – rather than in conflict with – the right to receive and impart information; this is actually the rationale underlying the draft EU Regulation on data protection, which explicitly sets forth the right in question. These issues are likely to be addressed, among other things, by the amendments to the Journalists' Code of Practice that are being worked out by representatives from the DPA and the categories concerned; one of the objectives of this drafting exercise consists

in adjusting the Code in force, which dates back to 1998, to the changes that have taken place meanwhile in media mechanisms.

*Online Politics*

Indeed, the risks arising out of the fact that major pieces of one's life are stored on the Net should be taken into account by having regard to data that are especially in need of enhanced protection because they have to do with a person's most intimate sphere, or because they lend themselves to being misused or may expose the data subject to discrimination. This is the case of the information concerning political opinions, which may be disclosed on the Net albeit with special precautions - as the Garante recalled in addressing cases that had to do with the voting mechanisms implemented for the "primary elections" of the centre-left coalition, in particular with the provisions concerning the need to undersign a "public call" and be enrolled in an ad-hoc "Register". Such provisions entailed the risk of disseminating sensitive data on the voters, as pointed out by some complainants. The Garante ordered the organizing committee to prevent dissemination of such data, especially on the Internet, by taking any and all measures that would be found appropriate for this purpose (decision of 31 October 2012, web doc. No. 2079275).

*Identity, Affectivity, Discrimination*

The peculiar criticalities brought about by the stepwise transfer to the Net of substantial portions of one's "private and public" life should not lead one to forget about the safeguards to be afforded to the personal data processed according to more conventional mechanisms – in particular whenever information deserving increased protection is at stake, such as the information on health, sex life or specific situations related to non-biological reproduction mechanisms.

Special importance should be attached in this regard to some decisions taken by the Garante in order to ban the disclosure, in certifications issued to unauthorized entities, of sensitive data that were not indispensable for the purposes of the administrative proceeding

concerned; in yet other cases the data at issue should not have been disclosed at all unless on the basis of a judicial authorization. In particular, a decision of 8 November 2012 prohibited a Registrar of Births, Marriages and Deaths from showing the full copy of the birth certificate relating to a person – now adult – containing a reference to that person's adoption.

Enhanced protection is also due to certain sensitive data that have to do with sexual orientation - including the evolution in time of such orientation. A significant example in this connection is provided by the decision whereby the Garante acknowledged an applicant's right to obtain, from the competent university, a new graduation certificate only showing the applicant's new data as taken from the census register after such data had been rectified in terms of the new sex attributed to the applicant – that is, without any reference to the reasons for the reprint of the said certificate (decision of 15 November 2012, web doc. No. 2121695).

## Discriminations and Violence

### November 2012 - January 2013 : Cyberbullying

**November 2012**: a fifteen-year-old boy from Rome committed suicide partly because of the sorrow caused by the unrelenting fun made of him because of his sexual orientation, especially on the Internet. In fact, a Facebook profile called "The pink-trousers boy" had been created on purpose.

**January 2013** – **Novara**: a fourteen-year-old girl committed suicide after being cyberbullied because she could no longer stand the jokes she had been the subject of over the previous days especially on SNS.

**January 2013 – Rome**: a sixteen-year-old boy attempted to commit suicide by throwing himself out of the window of the high school

class he attended, allegedly because of the jokes and bullying he was exposed to.

Thus, two suicides and one attempted suicide were reported by the media over barely three months – all of them concerning youths who were cyberbullied. According to a survey by the Italian Paediatrics Society (SIP), 34.2% of Italian teens have experienced cyberbullying or are friends with youths that have gone through such an experience.

**January 2013 – Rome. The Italian DPA on the right to have online information updated**

The Italian DPA ordered two publishing groups to implement a mechanism in their online archives such as to flag any developments in the news concerning a complainant; this was aimed at ensuring that the complainant's (current) identity would be respected as resulting from the thorough representation of facts involving him whilst enabling readers to receive reliable as well as thorough information – here, the fact that the complainant had been fully acquitted of criminal charges.

**October 2013 – Bergamo. Trading in medical data.** Some media reported on a sort of "sale" by health care practitioners of medical information concerning the patients admitted to the emergency department of a local hospital. This case was highlighted by the Italian DPA as well because it had to do, apparently, with the commercial exploitation of personal data held by reason of one's official duties; worse still, the data in question deserved special protection exactly because they could disclose the health of individuals and accordingly could expose such individuals to discrimination.

**2013. Measures taken by the Italian DPA against municipalities.** The Italian DPA issued inhibitory injunctions against about 30 municipalities in the course of 2013 as they had posted the names and diseases relating to individuals subjected to coercive medical treatments – the reason being that they had misinterpreted the

publicity obligations set forth in the current legislation. A similar misinterpretation accounted for the publication on the Internet by several schools of the names relating to the participants in a public competitive examination reserved for persons with disabilities.

**2013. Measures taken by the Italian DPA against public and private bodies in connection with the disclosure of biometric information.** Several inhibitory injunctions were also issued in 2013 against private and public bodies (including schools) that had relied heavily on biometrics systems to assess employees' attendance at work; such systems mostly collected fingerprints without any legal basis for such a processing, which should only be performed as a last resort measure. In one case the fingerprinting of employees for checking attendance at the workplace might have given rise to discrimination, given that the application lodged with the DPA referred to the use of such a system exclusively with regard to employees serving a sentence outside custodial institutions.

**2013. Measures taken by the Italian DPA against employers in connection with video surveillance of employees.** In terms of their number and importance, the inhibitory injunctions issued by the Italian DPA against several employers should be mentioned here; the employers in question had applied video surveillance to their employees without complying with the conditions set forth in specific legislation [Law No. 300/1970], i.e. without seeking the prior agreement of trade union representatives or obtaining an authorization from the Labour Inspectorate. These are breaches of provisions that were among the first ones to be introduced in Italy's legal system to protect privacy; indeed, there is such a power imbalance in this context between employer and employee that the data subject's consent is per se not enough as it might be easily coerced exactly on account of the employer's contractual power. This is why trade union representatives have to be involved or, if no agreement can be reached with them, an institutional authority is to be applied to such as the Labour Inspectorate.

The use of video surveillance in the absence of a legal basis is becoming widespread; in many cases no information is provided to data subjects in spite of this being a mandatory requirement. Even more serious are the cases where the cameras are hidden in such a manner as to prevent data subjects from realizing that they are being filmed.

**22 May 2013 – Ravenna. Video surveillance in nursery schools.** The Italian DPA banned the use of video surveillance in this context. As explicitly acknowledged by the nursery school, it had been introduced to "placate" parents more than on account of security considerations; the risk here was that, by so doing, children would be led to believe that it was "normal" to be under continuous surveillance – which might have also impacted the spontaneity of children's relationship with their teachers.

**24 May 2013 – Rome. "Wild" telemarketing.** Three injunctions were issued by the Italian DPA to impose fines amounting to Euro 800,000 on three major IT companies specializing in database management plus one telecom operator because of the breach of measures that had been issued against them in the past. It is often the case that personal data is processed unlawfully for telemarketing purposes even in respect of individuals that have signed up to the "opt-out register".

**June 2013. NSA interceptions.** Reports were published on the massive, indiscriminate collection of personal data and veritable "interceptions" carried out by the US National Security Agency, involving not only American citizens, on the basis of the special rules set forth in the Patriot Act (in particular, the Foreign Intelligence Surveillance Act) for anti-terrorism purposes. It is actually likely that data of European citizens have been acquired by US intelligence agencies, to the extent they had communicated with US citizens or used telecom services provided by US companies. This is due, at least in part, to the double standard that features in the applicable US legislation, which allows for derogations in respect of non-

citizens from the safeguards that are conversely applicable to US citizens vis-à-vis investigational activities. This sort of *ultra vires* operation of US legislation in Europe was the subject, among other things, of a working group set up by the Vice-President of the European Commission, Viviane Reding, as part of a broader review of the EU-US relationships with regard to mutually applicable data protection safeguards. However, the activities of this working group were considerably hampered by the reliance of the US counterparts on secrecy even concerning the interpretation of key concepts such as "foreign intelligence" – which were necessary to fully grasp the impact of Patriot Acts regulations.

**November 2013. Action strategy for the protection of European citizens' data.** An action strategy was developed by the European Commission and presented on 27 November 2013; the strategy envisaged, in particular, conclusion of the negotiations on an EU-USA "umbrella agreement" on the protection of personal data in the law enforcement sector by the summer of 2014 along with the strengthening of the EU-USA mutual legal assistance agreement of 2010 (including sector-specific agreements). The ultimate objective was to afford judicial remedies to European citizens and lay down an exhaustive list of the cases where European authorities may transfer data to US authorities including the relevant data retention periods and the terms for the use of such data. At all events, data transfers from European to US authorities might only take place in the cases expressly provided for in ad-hoc bilateral agreements. These provisions would be on the whole of the utmost importance because they would touch upon the main criticalities in the US legislation. The Commission's strategy also envisages the review, by the summer of 2014, of the Safe Harbor agreements that regulate the transfer of data to US companies; here the objectives include affording European citizens adequate remedies by way of alternative dispute resolution mechanisms in case of privacy breaches; enhancing the transparency of privacy policies so as to inform users (including non-US users) of the risks their data may be exposed to; strengthening oversight

by the US government on compliance with the agreement by the US companies also by involving the competent EU data protection authorities whenever non-compliance is allegedly at issue.

**November 2013 – Italy. Cybersecurity measures.** Special importance should be attached to the undersigning on 11 November 2013 of a memorandum of understanding – unprecedented in Europe – with the State's Intelligence and Security Department – allowing, inter alia, access by intelligence services to the databases of telecom providers – which also deals with the powers of intelligence agencies in the cybersecurity sector.

The MoU regulates specific as well as innovative information procedures, which are systematic in nature and regard the processing mechanisms for intelligence purposes in compliance with the precautions set forth in the data protection Code. This application of the powers vested in the data protection authority is better in line with the peculiarities that are currently a feature of the activities by intelligence agencies and their powers to "systematically access" information - which were expanded by Law No. 133/2012, partly further to a world-wide trend that is related to the growing risks from cybersecurity threats.

## Legislation and Policies

### *From Privacy to the Protection of Personal Data*

The right to the protection of personal data is not expressly grounded in Italy's constitutional charter. Obviously, the 1947 Constitution could not have included such right as we currently know it, i.e. as the right to informational self-determination.[1] Nevertheless, this right is currently covered by the Constitution, albeit indirectly, by way of the reference made in Article 117(1) to the EU's legal system, which

1 S. Rodotà, *La privacy tra individuo e collettività*, in *Politica del diritto*, 1974, 545.

includes Article 8 of the Charter of Fundamental Rights of the EU where this right is explicitly enshrined and the need is mentioned for independent authorities to enforce it.

The right in question is actually already set forth in the terms described above in Italy's legal system, even though based on statutory (rather than constitutional) provisions that implement Community legislation such as Directive 95/46/EC. Indeed, Law No. 675/1996 introduced a specific set of safeguards for the right to the protection of personal data although that right was not expressly laid down as such; at all events, a separate legal configuration was brought about for this right, other than that applying to the right to privacy which had already been linked to Article 2 of the Constitution by way of judicial decisions[2]. A highly peculiar type of protection was also introduced in this regard, i.e. one that is "relational" in nature.

The right to the protection of personal data was ultimately laid down as such in the data protection Code, which implicitly considered it to be part of fundamental human rights as well as being closely related to human dignity and personal identity – although this was done, once again, by way of a statutory rather than constitutional provision.

---

2 Reference can be made, in particular, to the judgments by the Court of Cassation in the Caruso and Petacci cases (Nos. 4887/1956 and 990/1963), where a shift took place in the privacy configuration scheme from a mainly negative dimension – the right not to have one's views altered – to a markedly positive, dynamic one, i.e. the "right to autonomous decision-making in one's relational life" and in the development of one's personality (see judgment No. 990/1963). The latter was traced back to Article 2 of the Constitution by having regard to the "full development of the human person" that is mentioned in Article 3, paragraph 1 of the Constitution. Reference can also be made in this connection to decision No. 139/1990 by the Constitutional Court, concerning the privacy protection rationale and, accordingly, the protection of inviolable human rights underlying the possibility to disclose statistical data exclusively in aggregate format; another decision by the Constitutional Court (No. 366/1991) had ruled that the findings of interceptions ordered in connection with a separate proceeding were not admissible as evidence: here privacy was considered to be a precondition for human dignity. This evolution of the privacy concept from the initial core notion of "false light in public eyes" was also fostered, prior to Directive 95/46/EC, by Convention No. 108/1981 of the Council of Europe; the latter introduced the concept of "data protection" as the right to the protection of private life against the automated processing of personal data, which was developed subsequently by the case-law of the European Court of Human Rights and traced back to Article 8 of the European Human Rights Convention (i.e. to the right to respect for private and family life) as construed in an evolutionary perspective.

This new right as enshrined in the Code was configured in a markedly positive perspective – namely, as a precondition to freely manifest oneself to the outside world, as the hard core of personal identity including its social dimension. In short, the right to the protection of personal data was set out as a prerequisite for human dignity and the free development of one's personality.

Whilst the protection of privacy is basically afforded by way of a static, negative approach as it is focused exclusively on the *jus excludendi alios* (the right to exclude the others), the protection of personal data has a substantially dynamic nature. Being construed as the right to informational self-determination, it empowers every individual to take steps vis-à-vis any entity handling their data and entails the possibility to lay down mechanisms and conditions for the processing of such data and to follow the data throughout their movements.

The features of the protection to be afforded are also different, since an increasingly preventive and case-specific approach is implemented and growing importance is attached to the collective dimension as opposed to an exclusively individual one – only think of the possibility for data subjects to be assisted by associations in exercising the rights set forth in Section 7 of the Code, modelled after the concept of collective protection of individual rights that is already enshrined in Law No. 300/1970 on employer-employee relationships. Furthermore, the protection in question relies on the interplay of procedural mechanisms that are grounded in both private and public law, which is once again modelled after European instruments.

*Scope of the Protection*

The right to the protection of personal data is vested, under Directive 95/46, in "natural persons" that are identified or identifiable (also indirectly) without prejudice to "the legislation on the protection of

legal persons with regard to the processing of the data concerning them" (see Recital 24). In transposing the directive, the Italian lawmaker decided to expand its scope of application to include legal persons, organisations and associations; this was a feature already of Law No. 675/1996 and was taken up by the 2003 Code. However, Section 40(2) of decree No. 201 of 6 December 2011 (so-called "Rescue Italy" decree) as converted, with amendments, into Law No. 214 of 22 December 2011 amended the text of the Code by excluding legal persons, organisations and associations from the scope of the protection at issue; it was considered that the extensive protection afforded by Italian legislation was an instance of gold plating and the amendments proposed would allow "a reduction in privacy-related costs" for businesses. In fact, this only applies to the processing of personal data concerning organizations, associations or legal persons as performed by companies, whilst it does not obviously regard the processing by such companies of data relating to natural persons. The ultimate effect produced by this reformation consisted actually in depriving legal persons and associations (including, for instance, political parties, NGOs, etc.) of whatever protection, so that the data concerning them may be processed without complying with the principles and procedural safeguards set forth in the Code.

The Italian DPA tried to remedy this *denegatio tutelae* (denial of protection) at least in part, by adopting an interpretive decision on 20 September 2012 whereby the sections in the Code concerning the processing operations related to the provision of electronic communications services may be applied further to the entities in question insofar as they are parties to contracts for the provision of such services – e.g. as for nuisance calls or unsolicited communications.

This interpretation would actually appear to be necessary in order to prevent conflicts with Recital 12 and Article 1(2) of Directive 2002/58/EC, which affords legal persons (to the extent they are subscribers to the services at issue) the protection applying to the processing of personal data in connection with the provision of

electronic communications services.

In spite of this significant reduction in the scope of the protection afforded by the Code, a bill was tabled by Government in the past legislative period whereby the scope of such protection would have been reduced further; in particular, the right in question would not be vested in individuals acting in their capacity as entrepreneurs, traders, handicrafts, or even "professionals" – that is to say, individuals performing whatever type of business activity. The "person" that, according to the Charter of Nice, is entitled to the "fundamental" right to the protection of personal data would have ceased thereby being the "natural person" as such and become the natural person "acting for purposes other than entrepreneurial, commercial, artisanal or professional activities" – i.e., the consumer as per the relevant definition in Legislative decree No. 206/2005.

Not too different is the wording contained in the governmental bill on simplifications (AS 958, Section 17), although the latter refers more appropriately to the data relating to *the performance of entrepreneurial activities.*

The scope of the protection afforded by the Code had been reduced further by Law No. 15/2009 (so-called Brunetta Law), which had amended Section 1 of the Code based on a proposal put forward by the then Junior Minister Ichino to exclude its application to the information concerning the performance and assessment of any person "discharging public duties". The impact of this amendment (which was repealed by way of Law No. 183/2010) was partly reduced by a provision introduced thereafter (via Section 19, paragraph 3a, which is now part of legislative decree No. 33/2013), whereby public administrative bodies are required to disclose the above information except for such items as may allow inferring sensitive data.

*The Individual and Marketplace*

The aforementioned legislative amendments mirror two trends that

are becoming increasingly significant in the legislative policies applying to this sector.

One of them has to do with the stepwise reduction in the scope of application of data protection legislation as regards business and production activities – starting from decree No. 70/2011, which markedly downsized the protection of personal data in business-to-business relationships. There followed the exclusion of legal persons and – which was perhaps unintended by lawmakers – organisations and associations from the scope of the data protection right, plus the proposal for excluding natural persons exercising commercial, entrepreneurial or professional activities.

This trend towards reducing the scope of privacy for the sake of market requirements is also mirrored by the shift from opt-in to opt-out in telemarketing activities pursuant to decree No. 135/2009 as converted, with amendments, into Law No. 166/2009. This means that whoever does not wish to be contacted for marketing purposes is now required to sign up to an ad-hoc "opt-out register", whilst the opposite rule was applicable beforehand – i.e., the data subjects' prior informed consent was necessary in order to contact them.

In no way different is the rationale underlying the elimination of the so-called security policy document from the minimum security measures to be taken by data controllers, as per decree No. 5/2012. Whilst the drafting of such a document was probably a disproportionate requirement in respect of some processing operations and was in any case poorly helpful in a preventative perspective, it might have been replaced at least by other measures – perhaps less daunting but sufficiently effective.

The concept that is ultimately shared by all the above measures is that privacy means costs for businesses and such costs must be reduced as much as possible – especially at a time when economic crisis is so rife; a passage in the Explanatory Report to the bill for enacting the decree No. 201/2011 is especially significant in this regard. This is obviously a misrepresentation – not only because a fundamental

right, far from being a cost, is actually an asset: as stated by Jean Paul Fitoussi, violating rights is cost-ineffective. But this is so also because the stepwise reduction in the scope of the protection afforded by the Code has ended up harming companies, as shown by the interpretive provision issued by the Italian DPA with regard to decree No. 201/2011 – which was made necessary to prevent legal persons from being deprived of whatever protection against wild telemarketing or nuisance calls unlike all other subscribers to electronic communications services.

In order to prevent these unintended consequences and avoid that the right to the protection of personal data becomes – like so many other fundamental rights – a market-dependent variable, one should on the one hand raise the awareness of the importance of these rights, and in particular of the right to privacy that is as yet overlooked as a fundamental precondition for one's freedom; on the other hand, one should refrain from viewing, regulating and depicting these rights merely as red tape, as corporate costs to be borne in order to comply with complicated, hyper-detailed procedures that are poorly understandable in terms of their import, value and function.

This is especially the case with personal data protection legislation, which is today (as yet) excessively focused on compliance with requirements that are as stringent as they are theoretical in nature – so that they are all too often breached, which accounts for the poor effectiveness of the legislation at issue. This is shown most clearly by the number of sanctions imposed by the Italian DPA on account of violations that consist exclusively in the failure by data controllers to fulfil basic obligations: failure to provide information notices; failure to obtain consent; failure to adopt minimum security measures. A substantial portion of those sanctions result, on the other hand, from the breach of obligations related to the powers vested in the DPA: failure to notify processing operations to the DPA; failure to provide information to the DPA; failure to comply with measures taken by the DPA. The amount of the pecuniary sanctions imposed is also significant, since upper and lower thresholds as set out in the law

are considerable and do not always mirror the detrimental impact of the facts at issue. Moreover, criminal and administrative penalties may be imposed cumulatively, pursuant to a specific provision in the Code; in case of multiple wrongdoings (even of the same type), sanctions are imposed cumulatively rather than by taking account of the highest possible sanction for the most serious wrongdoing; and the violation of certain provisions in the Code is construed to give rise to a separate wrongdoing, of a derivative nature (see, for instance, Section 164a, paragraph 2), for which a sanction is imposed on top of that applying to the "primary" wrongdoing. Indeed, that so many violations of data protection legislation are still committed despite such stringent sanctions cannot but lead one to consider either that the applicable obligations are basically unknown or that such obligations are, if not inapplicable, at least disproportionate - i.e., unreasonable. In either case, there is clearly the need for considering how appropriate the legislation in force is to address an ever-changing reality; this is ultimately aimed at preventing a wider gap than the one currently existing between statutory provisions and compliance. Preference should be given as much as possible to solutions that take due account of the specific features of the case at hand without relying on general, theoretical assumptions.

The DPA is actually endowed with tools that enable it to move in that direction, ranging from the balancing of interests as a tool to exempt from consent to the quasi-regulatory powers (general authorisations, guidelines, prescriptive measures addressed to whole categories of data controller) whereby it can adjust the rules as much as possible to the peculiar features of each processing operations also via simplification measures – which has actually been the case repeatedly. Still, these tools prove effective to a limited extent in the absence of in-depth changes to the system as a whole.

In fact, the widespread use of technologies that entail the processing of data and the multifarious contexts in which an individual may be "tracked" to a more or less considerable extent make it necessary for legislation to be increasingly flexible and practical in order to

become as adjustable as possible to the specific contexts. Provisions are required that enable courts and administrative authorities, and in particular the Italian DPA, to take due account of the peculiarities of each case at hand.

Of course, this does not mean that the right in question should give way even more to conflicting interests such as those coming from the marketplace, businesses, etc.; in fact, it means that requirements that go mostly unmet and are probably of little help should be replaced by other, more reasonable, effective requirements. One could envisage, for instance, ad-hoc regulations for biometric data that do not legitimate the wide-ranging use of this technology, often unjustified, but rather adjust the general assumption on the disproportionate nature of the processing of such data by having regard to the specific type of biometric data and the resulting risks to data subjects. There is little doubt that the risks arising out of fingerprinting or the use of vein pattern or graphometric analysis are quite different from those related to facial images. By the same token, the actual decision-making power and autonomy of an employee giving his or her consent to the taking of fingerprints in order to check attendance at the workplace are definitely different from those vested in the customer of a bank. There is clearly the need to appropriately regulate the preconditions to consider that consent is valid, as consent may never be coerced or conditional; account must be taken of the contractual relationships and/or the context where consent is provided with particular regard to the imbalance in the parties' contractual power – especially in the employer-employee relationship. It is no chance that Law No. 300/1970 was the first piece of legislation that introduced, in our legal system, provisions to protect privacy apart from those laid down in the Criminal Code – exactly to protect employees against undue interference by employers and forms of surveillance at the workplace such as to violate their dignity. This is why trade union representatives were empowered to step in given the excessive weakness of the individual employee.

*Transparency in public administration and opacity in private life*

The Ichino amendment referred to above provides a very topical example of the trend in the public sector to downsize privacy for the sake of the increased transparency in public administration.

From this standpoint, the evolution of the transparency principle is especially significant, starting from its being set out as a general principle of administrative activity in Law No. 15/2005 up to the provisions made in the Brunetta Laws (Nos. 15 and 69 of 209, and legislative decree No. 150/2009) where transparency is construed as "total accessibility" to several data concerning activity and organization of public administrative bodies; this is instrumental to the "public oversight over compliance with performance and impartiality principles" – i.e., exactly the oversight that is not the ultimate objective of the right of access under Law No. 241/1990 [Italy's Freedom of Information Act].

The non-procedural nature of the civic access right introduced by legislative decree No. 33/2013 is all the more evident; under this right, every citizen is entitled to access such data and information as public administrations failed to disclose even though they were required to do so. This new type of access is not grounded in a vested interest as it results from the need for democratic oversight on the activity of public administrative bodies – which is exactly why no case-by-case balancing is required with the right to privacy of the counterparts, contrary to what is the case with the freedom of information provisions laid down in Law No. 241/1990. This is also the reason why the DPA recalled, in its opinion on the said legislative decree of 2013, that the information to be posted on the Net should be selected appropriately by having regard to its being instrumental to ensuring democratic oversight on public administration, whilst the visibility of personal data should be limited to what is absolutely indispensable - especially if sensitive data are involved. Significantly, the DPA requested in its opinion that any data disclosing information on a person's health or financial or social distress situations should

be exempted from the mandatory disclosure obligations set forth in respect of allowance-related measures – e.g. exempting certain individuals from payment of school canteen fees or health care fees based on the presence of specific diseases or income bracket rules.

The above guidance is far from being redundant. Only think, for instance, of the substantial investigations that led the DPA to issue inhibitory injunctions against several municipalities that had posted, on their websites, orders for coercive medical treatments (*trattamento sanitario obbligatorio, tso)* including the personal data of the relevant addressees and the respective diseases. There is little doubt that publishing this information is not only unlawful, because it is breach of the ban on disseminating health care data under Section 22(8) of the data protection Code, as well as serving no transparency objectives, since it does not shed any light on the exercise of administrative powers; in fact, it is dangerous for the individuals' dignity, because it can disclose data that are liable to expose those individuals to severe forms of discrimination and may remain on the Net without any possible constraints.

Similar measures were taken by the DPA with regard to the publication on the Net of the names of participants in public competitive examinations reserved for persons with disabilities; such a publication was in breach of the data subjects' dignity and was in no way instrumental to public oversight on public administration.

It is no chance that the ban on disseminating health care data, which was breached by the aforementioned publication, is aimed at protecting data subjects exactly against the most diverse forms of discrimination and social stigma that might result from an ill-conceived notion of transparency and "glass-house administration". In short, transparency does not mean posting all the data relating to an administrative proceeding on the Net, since there might be information that is irrelevant to public oversight on the exercise of public powers and may, above all, prove detrimental, at times irreparably so, to individuals' dignity. Transparency should be a

driver of democracy, not a means to violate human dignity.

From this standpoint, focusing unrelentingly on the relevance of the information to be disclosed for the purpose of the democratic oversight on public administration can allow turning privacy and transparency into complementary, rather than conflicting, assets – as both are necessary to ensure the rule of law in a State, like ours, grounded in democracy, pluralism, a presumption in favour of safeguards and the protection of the individual.

*Freedom and Security*

A similar relevance benchmark should be applied to the processing of personal data for public security purposes, partly on account of the sector-specific features of the relevant legislation. The latter entails a significant reduction in the safeguards afforded to data subjects and was recently expanded in scope following policies that increasingly prioritise security and have considerably enhanced the information-gathering powers of law enforcement bodies (as well as of intelligence agencies). Reference can be made, for instance, to the authorization granted to municipalities by decree No. 11/2009 to rely on video surveillance systems in public or publicly accessible places for the rather vague purposes of "urban security"; to the access by intelligence services to the personal data held by providers of electronic communications services in order to ensure "cybersecurity" as per the Prime Minister's decree of 24 January 2013; to the "preventive" interceptions of telephone, Internet and environmental data that intelligence services and administrative authorities are empowered to carry out upon the public prosecutor's authorization with a view to preventing certain criminal offences under Section 226 of the implementing provisions of the Criminal Procedure Code – which powers were expanded further by Law No. 133/2013; to the exchanges of sensitive, judicial, even genetic data relating to suspects of crime between Italian and US law enforcement authorities pursuant to the Agreement of 28 May 2009

on the strengthening of cooperation in preventing and countering serious forms of crime, which has yet to be ratified; to the envisaged creation of a national DNA database as per the Law ratifying the Treaty of Prüm (Law No. 85/2009), where the genetic profiles acquired in the course of criminal proceedings will be stored along with those of individuals placed under measures limiting personal freedom, to be then accessed by police and judicial authorities for purposes of international law enforcement cooperation; to the so-called freezing, that is the storage of Internet traffic data upon an order issued by the police – to be validated subsequently by a court – for preventive purposes; finally, to the lack of specific regulations on the admissibility at trial of images filmed in private dwellings, which the Constitutional Court could not include under the scope of interception-related legislation because no indications came from Parliament in this regard.

The above processing operations touch upon highly sensitive data including judicial and genetic data; this is why it is all the more important to limit the information-gathering powers of law enforcement authorities to such data as is actually indispensable for preventing or detecting very serious crimes and by implementing procedural mechanisms that must be subject to full judicial review. Similar safeguards should apply to the processing performed by intelligence agencies, partly in the light of the broader intelligence-gathering powers conferred on them by Law No. 124/2007 and in particular following the amendments brought about by Law No. 133/2013. The latter provided actually the foundations for the so-called "Monti directive" of 24 January 2013, whereby intelligence services were empowered to access the databases of the providers of electronic communications services to protect "cybersecurity". One should also consider that, in addition to the review carried out by the Copasir [a parliamentary oversight committee] on the activities of intelligence services (from both a political and a legitimacy standpoint), the Italian DPA is empowered to carry out inspections into the processing of personal data by such services to

establish conformity with the applicable principles – which include relevance, lawfulness, fairness, and legitimacy of the processing. The implementing procedures ought to have been set out in an ad-hoc decree by the Prime Minister's Office (under Section 58(4) of the Code), which however has yet to be issued.

Respect for the relevance principle should serve all the more as a key element in regulating access to personal data by administrative authorities in order to counter non-criminal wrongdoings: this is the case, for instance, of the communication to the Revenue Office of the data concerning the financial operations of all Italian citizens as provided for in decree No. 201/2011 to foster the fight against tax evasion and elusion.

One should also reiterate the need for ensuring that those individuals that are subjected to the State's authority are made aware of and can effectively profit from the right to the protection of their personal data.

This applies in particular to the inmates of prisons or custodial establishments, and to the aliens detained in the Identification and Deportation Centres (*Centri di identificazione ed espulsione*, C.I.E.), since "the fragility of their situations and circumstances might make them truly "naked" vis-à-vis public authority" and lead them to more easily waive even fundamental rights – which may not be overridden, not even *in vinculis* [when one is in chains] (see the DPA's Report to Parliament for the year 2012).

*Media and Privacy*

An issue that is continuously under the focus of Parliament, to little avail, has to do with the relationship between privacy and media; this issue is usually addressed from the "trial by the media" standpoint, i.e. in terms of the disclosure of investigational records and, in particular, of wiretap transcripts. Given this background, the right to privacy vested in the parties to a judicial proceeding as

well as in any third parties concerned by the relevant investigations is relied upon instrumentally as an excuse to legitimate significant limitations on the use of the above tools for the taking of evidence; this is especially so in the governmental decree that was approved during the past legislative period, albeit not yet finally. As shown by the many cases addressed by the DPA, one should rather introduce more stringent safeguards for those individuals that deserve increased protection – such as children and the victims of crime – as well as in order to ensure full respect for the presumption of innocence principle; to that end, one should make sure that judicial developments are mirrored in the news reported on the media. It is often the case that a defendant depicted as guilty of the most heinous crimes in the headlines is then acquitted of all charges, but this piece of information fails to be given the same emphasis.

As suggested by the DPA, it would also be appropriate to update the Journalists' Code of Practice, which provides the benchmark in assessing whether data is being processed lawfully. Over fifteen years elapsed since it was first adopted, and the current multiplication of information sources makes it increasingly necessary for professional ethics to be careful not to mistake what is in the public interest by what is interesting for the public. By drawing inspiration from the provisions made in the draft data protection Regulation that is being discussed at EU level, one should lay down specific safeguards to protect the data subjects' right to be forgotten; for instance, one might require – as was done by the DPA as well as by judicial authorities and the ECHR – that the information (especially on judicial proceedings) stored in the online archives of media be de-indexed and/or updated, partly on account of the risks for the data subjects' dignity that are made more poignant by search engines and their autocomplete functions.

## Recommendations

1. Including organizations and associations into the scope of the data protection right. This reformation might be counterbalanced by a general re-haul and update of the requirements applying to data controllers under the Code.
2. Revising the framework of the sanctions envisaged in the Code as regards both administrative wrongdoings and criminal offences by way of an in-depth reformation along the following lines: derogations should be excluded from the principle whereby administrative wrongdoings can cover criminal offences; proceedings for the offence of unlawful processing of personal data should be instituted on the basis of a complaint lodged by the victim; several wrongdoings consisting in non-compliance should be de-criminalised as they are not prejudicial to third parties; additional non-punishability clauses should be included for both administrative wrongdoings and criminal offences based on the offender's or wrongdoer's remedial actions and compensatory measures.
3. Expressly excluding any data disclosing information on health or specific situations of economic or social distress from the disclosure obligations applying to personal data as grounded in the transparency requirements regarding public administrative bodies.
4. Introducing ad-hoc regulations in respect of the processing of biometric data. Such regulations should in no way legitimate the blanket reliance on such data that is currently a feature, in particular by laying down the necessary preconditions to consider that data subjects' consent is really free.
5. Implementing the provisions contained in Section 53 of the Code; the latter requires a decree by the Minister of the Interior to implement a "census" of the databases set up for public

security purposes so as to enable data subjects to exercise the rights afforded by the Code also in this area in order to protect their own personal data. Furthermore, stringent provisions must be laid down to regulate application of the Code to intelligence activities.

6. Introducing legislation to limit the use of personal data by law enforcement authorities (especially if sensitive, judicial or genetic data are involved) to such data as is absolutely indispensable to pursue the prevention and detection of especially serious crimes and to the extent the use of such personal data can actually ensure effective prevention.

7. Providing in the regulations to be issued with regard to the national DNA database that the retention periods of genetic profiles should be adjusted to the relevance of such genetic information for the specific purposes of the investigations into the individual criminal offences.

8. Introducing, as called for by the Constitutional Court and by the Court of Cassation, specific regulations regarding admissibility at trial of images filmed in private dwellings. To that end, the regime applying to the interception of communications should be extended expressly to such filming if it is such as to enable the "capturing" of conversations. In particular, it would be appropriate: 1) to regulate and limit the recording of conversations unbeknownst to the persons concerned, which is considered lawful so far; 2) to update Journalists' Code of Practice by also laying down additional safeguards for those individuals that deserve enhanced protection, such as children and victims of crime, as well as to ensure full respect for the presumption of innocence principle; 3) to lay down specific measures to afford data subjects the right to be forgotten.

9. Making sure that the right to the protection of personal data is implemented effectively in all places where individuals are deprived of their freedom - by raising the awareness of

this right among prison inmates, persons held in custodial establishments, aliens detained in C.I.E. .