Emerging contours of data protection as a universal human right

By Jörg Polakiewicz

Introduction

I vividly remember the panel at the closing session of last year’s conference in Mexico City. Speakers from North America were very sceptical about a human rights approach to privacy and data protection, arguing that concepts differed so much that it was impossible to come up with any global standards in this field. Efforts should instead focus on interoperability between regional approaches. The European panellists on the other hand stressed that any discussions on data protection regulation worldwide should start from the premise that it is a universally recognised human right.

Are there internationally agreed standards of the right to privacy and data protection?

The right to privacy and data protection is guaranteed under the International Covenant on Civil and Political Rights (ICCPR)

1 Professor at the Europainstitut of the University of Saarbrücken and Head of the Human Rights Policy and Development Department, Directorate General of Human Rights and Rule of Law, Council of Europe. This report was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe
and European Convention on Human Rights (ECHR). It has been introduced as a fundamental right in constitutions all over the world and in the EU Charter of Fundamental Rights. Constitutional and supreme courts all over the world as well as the European Court of Human Rights and the Court of Justice of the European Union have developed strict conditions for the collection and processing of personal data.

The European Court of Human Rights held that “the storing by a public authority of information relating to an individual’s private life amounts to an interference within the meaning of article 8. The subsequent use of the stored information has no bearing on that finding.”

Some examples from that Court's case law illustrate the very practical consequences:

- Any state interference is subject to a proportionality test. Any storing, but also the processing and sharing of personal data must be “in accordance with the law”, pursue legitimate aims and, in addition, be “necessary in a democratic society” to achieve those aims.

---

The requirement of a legal basis for any state interference is particularly relevant. It means for example that the *retention of personal data requires a legal basis* and must be proportionate to the legitimate aim pursued. This is the reason why European data protection commissioners recently objected against the requirement, proposed within **ICANN**, for registrars to **retain data of domain name holders** (telephone numbers, email addresses) for a period of two years after the contract for the domain has been ended.³

- Even **public information** can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.⁴

- The state is required to create an **appropriate regulatory framework**, including both **legislation and enforcement capacity**, to ensure effective protection for individuals whose data are collected and processed, also vis-à-vis interferences by nonstate actors.

- State authorities must not establish secret surveillance security database; **people have a right to know why they are registered, and what type of information is**

---


⁴ Rotaru v. Romania, § 43, 4 May 2000
included and for how long, how it is stored and used or who has control over it.\textsuperscript{5}

- There must be \textbf{accessible and effective remedies} not only to challenge the storage and use of personal data, but also to secure the destruction of the files or the erasure or rectification of unlawfully stored information kept in them.\textsuperscript{6}

As regards the last point, it is interesting to note the preliminary findings of a recent \textbf{European study on redress mechanisms in the area of data protection}. Victims of a data protection breaches appear to have been reluctant to seek redress in court, due to formalities, costs, delays and uncertainties, but also because of a general tendency to restrict the possibility of seeking compensation for a violation of data protection rights, due to strict procedural and evidence related requirements.\textsuperscript{7}

\textbf{Interferences by private actors}

The idea of human rights protection, which has found its expression since the 18\textsuperscript{th} century in bills of rights, constitutions and international human rights treaties, has primarily been developed and conceived for the relationship between \textbf{citizens}

\textsuperscript{5} Shimovolos v. Russia, 21 June 2011.

\textsuperscript{6} Segerstedt-Wiberg and Others v. Sweden, 6 June 2006.

and state authorities. In a world where states were the only actors and subjects of international law, “the public domain, the interstate sphere, and the realm of governance were largely coterminous.”

While nonstate actors may not violate human rights, their activities may interfere with those rights to such an extent that state action may become necessary to ensure effective protection. **Positive obligations** ("Schutzpflichten") of states to protect privacy rights have always been central in the development of data protection regulation. Already back in 1981, when Convention 108 was adopted, there was agreement to apply its **principles to the public as well as the private** sector. Already then most data traffic occurred in the private sector. During the last thirty years, this reality has not changed, only the availability of personal data and the technical capacities to collect and analyse them have increased exponentially, in particular through the internet. Today it is possible for companies like Google to **collect and analyse in real time traffic data of millions of internet users** and to make them available **for commercial purposes**, while a similar collection by public authorities for law enforcement purposes would be prohibited under the laws of many countries. States have **positive obligations** to ensure, through appropriate legislation which reconciles the different

---

private interests and rights at stake, that such powers are not abused. Its horizontal scope of application is one of the strengths of Convention 108.

**Is all this too European for the global market place?**

I do not think so. Latin American legal traditions are certainly close to our European ones. Several countries, notably **Argentina, Brazil, Colombia, Mexico, Peru and Uruguay** have a constitutional right to data protection. The 1988 Brazilian constitution was the first to introduce the right to an effective remedy (*habeas data*). In its remarkable judgment C-748/2011, the **Colombian Constitutional Court** reviewed the constitutionality of implementing legislation, adopting a deliberately comparative law approach. The proposed legislation, which has been enacted on 17 October 2012, provides for previous, express and informed consent for data processing.

Their **Northern American neighbours** traditionally think of privacy as a right against government intrusion, with the fourth amendment jurisprudence as a robust baseline. In **United State v. Jones**, the Supreme Court held that the government's installation of a GPS device on a car, and its use

---

of that device to monitor the vehicle's movements (for 28 days), constituted a "search". Though the majority did not address whether that search was unreasonable and required a warrant, the US Solicitor General called the decision "a signal event in fourth amendment history", since according to the previous case law, a person travelling by car on public thoroughfares has no reasonable expectation of privacy. The idea of "reasonable expectation of privacy" is by the way not alien to European thinking. The European Court of Human Rights used it notably in Peck v. United Kingdom. However, the fourth amendment does not appear to offer much protection vis-à-vis privacy intrusions by private corporations. In the absence of generally applicable legislation, US privacy rights with respect to private companies remain for the time being limited. Wireless or smartphone companies are not prohibited from disclosing to third parties a detailed record of their customer's traffic data. There appears to be no law that prevents a web browser from sharing an individual's browsing history with its business partners, or a social network from taking the photos posted online to share with friends and using them to generate a precise and unique


personal profile. All this may of course change if the United States enact the comprehensive **privacy bill of rights**, as proposed by the Obama administration.

The situation is similar in many **Asian countries**, where some pretend that the human rights discourse is Western and irreconcilable with traditional values. And yet, human rights have been articulated no less often in Asia than in Europe.\(^\text{12}\)

Courts in that region use increasingly the notions of necessity and proportionality. On 23 August 2012, the **South Korean Supreme Court** declared the country’s **internet ‘real name’ policy** unconstitutional, arguing that the freedom of speech can be regulated only when it is clearly beneficial to the public: “Despite the enforcement [of the real-name system], however, there has not been a significant decrease in illegal or malicious postings online ... If we are to restrict freedom of expression, the public interests we would thereby protect and acquire must be clear ... The policy has caused reverse discrimination between domestic (local websites subjected to the law) and overseas businesses. Taking these factors into consideration, it is difficult to say that we have contributed to public interest.”

---

How does Convention 108 seek to secure effective protection for the right to privacy and data protection?

The purpose of Convention 108 is to secure respect for the right to privacy for every individual. The choice of “privacy” rather than “private life” is not a coincidence. Already in 1981, Convention 108 adopted a deliberately international approach, reaching out beyond Europe. As the explanatory report notes “[i]t does not seem advisable ... to rely solely on the European Human Rights Convention for data protection, inter alia because it is a ‘closed’ instrument, which does not permit the participation of non-European and non-member states.”13

The question of the nature and scope of the right to data protection has resurfaced again during the Convention’s modernisation process launched in 2010 with the full support of European Ministers of Justice.14 It pursues two main objectives:

- to deal with challenges for privacy resulting from the use of new ICTs, echoing the concern that modern information


and communication technologies enable observation, storage and analysis of most day-to-day human activities, more easily, rapidly and invisibly than ever before, thereby potentially creating a feeling of being permanently watched, which may impair the free exercise of human rights and fundamental freedoms;

- to strengthen the Convention's follow-up mechanism.

The Convention's preamble originally referred only to “everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy.” Now it is proposed to add the notions of “human dignity” and “the right to control one's own data and the use made of such data.”

Whereas supporters of this proposal consider that control of information is an important aspect of data protection, derived from the right to privacy, others, in contrast, take the view that this inclusion might be confusing, giving the impression that a new right was being established.

The idea of control over one's personal data is inherent in the notion of “the right to informational self-determination” (“Recht auf informationelle Selbstbestimmung”), which the

---

15 See the most recent proposals for the modernisation of Convention 108 contained in document T-PD(2012)04 rev2 en (16 October 2012), at: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp which will be examined at the forthcoming plenary meeting of the conventional committee T-PD on 27-30 November 2012.
German Federal Constitutional Court derived not from the right to respect for private life, but rather from the right to the free development of personality. In its landmark 1983 decision, it stated that privacy is not only an important fundamental right but also a precondition to a democratic society.

Before dealing more in detail with the question of balancing of competing rights, I would like to mention two other features of the revision process that are directly related to human rights concerns:

- the treatment of sensitive data,
- accountability and transparency

**Sensitive data**

Convention 108 required special safeguards for a non-exhaustive list of “special categories of data”,¹⁶ the processing of which was considered particularly likely to lead to encroachments on individual rights and interests. The original list referred to data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and also data relating to criminal convictions.

In the modernisation process, it is proposed to add genetic data, trade-union membership, as well as data processed for the identifying biometric information they contain. More

---

¹⁶ Article 6 – Special categories of data.
importantly perhaps, it will be recognised that the risks for persons depend not so much on the contents of the data but on the context in which they are used. It will also be specified more clearly than in the original Convention that the additional appropriate safeguards which are required for the processing of such data must prevent the risks to the interests, rights and fundamental freedoms of the data subject.

**Transparency, impact assessment and privacy by design**

The proposed amendments to Convention 108 also foresee new obligations regarding the **transparency** of processing, **impact assessment** and **privacy by design**. Controllers will be required to carry out a risk analysis of the potential impact of the intended data processing on the rights and fundamental freedoms of the data subject and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms. **Privacy by design** should ideally be implemented across the board, in IT systems, through accountable business practices and networked infrastructure. The idea is to move from a reactive to a proactive mode.

I would like to emphasise that those additional obligations correspond to requirements established under the **APEC Privacy rules**, thus representing a truly international approach. To be meaningful and cost-effective, the

---

17 New articles 7bis and 8bis.
requirements will of course have to be scaled and adapted to the size of the processing entity, the volume of data processed and the risks at stake.

We are convinced that, once a **culture of privacy** exists within an organisation, consumer confidence and trust will increase and opportunities to build business and competitive advantages will follow naturally.

**Balancing of competing rights and freedoms**

What makes the regulation of data protection such a delicate task is the necessity to **strike the right balance between the right to data protection and various other fundamental rights and freedoms**, such as the freedom to receive information (especially that of internet users), freedom of expression (the ‘press privilege’), the freedom to provide services, the right to property and to conduct a business, workers' rights in the context of employment and collective action, freedom of association of trade unions and political parties (in the context of collection of ‘sensitive data’).

Rights of the same rank have to be weighed against each other, ideally reconciled *in casu*, in line with the principle of proportionality. One guiding idea is what we call in German *“praktische Konkordanz”* (‘practical reconciliation’). The term was coined in the 70s by Konrad Hesse, judge at the Federal Constitutional Court of Germany. According to this principle,
one right cannot overtake the other; both must be considered of equal importance. The balance should be conducted while trying to satisfy both rights, so that the limitation on the first right is equal to the limitation on the second one, taking into account the circumstances of each case.

The European Court of Human Right's case law on privacy provides numerous examples of such balancing tests. Cases related to the publication of personal data, such as photographs\textsuperscript{18} or video footage\textsuperscript{19} but also to the protection of minors.

In the case of \textit{K.U. v. Finland}, the Court highlighted the need to protect victims of cyber-bullying. The then 12 years old applicant had been contacted following the publication by unknown persons of an advertisement on a dating site on the internet, which mentioned his age and year of birth, gave a detailed description of his physical characteristics, a link to the web page he had at the time which showed his picture, as well as his telephone number. The advertisement stated that he was looking for an intimate relationship with a boy of his age or older "to show him the way". When asked to identify the person who had placed the advertisement, the service provider refused to reveal the identity of the holder of the IP address in


\textsuperscript{19} See for example: ECtHR, \textit{Peck v. United Kingdom}, No. 44647/98, 28 Jan 1993 or ECtHR, \textit{Mosley v. United Kingdom}, No. 48009/08, 10 May 2011.
question, referring to the confidentiality of telecommunications protected under Finnish law.

The Court rejected this argument: “Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.”

In the Mosley case, the applicant’s sexual activities were published in a newspaper and on its website. Mr Mosley wished to enforce a duty for newspapers to notify subjects of future publications prior to publication. The Court held that “the protection of article 10 ... may cede to the requirements of article 8 where the information at stake is of a private and intimate nature and there is no public interest in its dissemination.” It rejected, however, the idea of a legally binding pre-notification requirement having regard to the “chilling effect” to which a pre-notification requirement risks giving rise, to the significant doubts as to the effectiveness of

---

20 European Court of Human Rights, K.U. v. Finland, judgment of December 2, 2008 (no. 2872/02), § 43.

21 ECtHR, Mosley v. the United Kingdom, No. 48009/08, 10 May 2011, para. 131.
any such requirement and to the wide margin of appreciation in this area.

The Court has also set out a series of general criteria delineating the extent to which media companies may interfere with privacy rights:²²

- Contribution to a debate of general interest;
- How well known is the person concerned and what is the subject of the report?
- Prior conduct of the person concerned;
- Content, form and consequences of the publication;
- Circumstances in which the photos were taken;
- Severity of the sanction imposed.

The relationship between data protection and freedom of expression is also being debated during the modernisation process of Convention 108. Representatives of the media industry asked for a “robust exemption for processing of personal data for journalistic purposes.”²³ We have not gone so far. However, the current draft amendments recognise freedom of expression as a valid ground to restrict

---

²² In two Grand Chamber judgments of 7 February 2012, Axel Springer AG v. Germany and Von Hannover v. Germany (no. 2).

²³ European Magazine and Media Association & European Newspaper Publisher’s Association ENPA & EMMA), T-PD(2012)04Mos of 12 June 2012, 165.
certain of the principles guaranteed under the Convention, including those governing transborder data flows.

Freedom of expression was also invoked as a reason not to include a specific “right to be forgotten” among the amendments proposed for the modernisation of Convention 108. It was felt that the rights of rectification or erasure and opposition, together with the provisions restricting the length of data storage would offer a sufficiently effective protection to the data subject.

**Conclusion**

We are currently at risk, more than ever before, to lose control over our personal information. People in George Orwell’s famous novel ‘1984’ were constantly reminded that they were under complete surveillance. We should remind ourselves that through our interconnected way of life, we continuously expose essential aspects of our private life.

But let us not despair; rather let us unite the “pessimism of the intellect with the optimism of the will”. Data protection regulation has always been developed in reaction to technological development.

---

24 Antonio Gramsci.
Privacy in the sense of the **right to be left alone** may not be understood in the same way by individuals living in places as diverse as Dakar, Montevideo, Oslo, Shanghai or Tokyo. However, in spite of widely differing cultural and legal traditions, we should be able to agree on **one essential dimension of privacy**, the **right to the protection of personal data**. The contours of a universal right of every person to decide how his or her personal information is collected, used and distributed are clearly emerging.

**Thank you for your attention.**