1 Protecting the Individual in Front of Technology

The right to respect for private life recognises in arguably rather general, vague terms the right of individuals to be protected against unjustified, disproportional or arbitrary interferences in their private and family life, their home and their correspondence. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 4 November 1950 is written in such terms, but fails to define how the mentioned private and family lives, home or correspondence should be understood. Neither does it explain what is exactly

1 Art. 8 of the ECHR: “1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

2 It will be noted that Art. 8 of the ECHR does not mention the term ‘privacy’, but refers to the right of respect for one's private life. This notion, which has been developed over the years by the European Court of Human Rights in an activist fashion, has an open and evolving nature: thus, it has been judged that it may be not only impossible, but also useless to define it (Rigaux, F. (1990), La protection de la vie privée et des autres biens de la personnalité, Bruxelles, Bruylant, p. 725). The notion is related to, but not fully coincidental with the notions of ‘privacy’ as conceived by American or British legal frameworks. The notion of ‘privacy’ has been extensively debated from different perspectives (see, notably: Schoeman, F. D., (Ed.) (1984). Philosophical Dimensions of Privacy: An Anthology. Cambridge: Cambridge University Press), and should in any case also be considered as referring to a plurality of values (on the relation between both notions, see, among others: Hildebrandt, M. (2008). Profiling and the Identity of the European Citizen. In Hildebrandt, M. and S. Gutwirth (Eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives (p. 303-343), New York: Springer).
meant by interferences with them. It is the judiciary and the legislator who have been working out, over the years, the interpretation of the content of the right, eventually distilling and constructing a series of much more concrete legal instruments and concepts through which it is to be applied and guarded.

One of the major challenges of such translation of the right into more easily applicable legal tools has consisted in the taking into account of technological developments. Since the 1960s, and especially during the 1970s, it has been felt that, for the right to respect for private life to offer sufficient guarantees for the individual in front of such developments, special attention needed to be granted to the automated processing of personal data. This notably lead to the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, as well as of many other legal instruments focusing on the regulation of the processing of personal data. The vitality of this approach has been so strong that the protection of personal data progressively became a model for privacy protection, and even managed to establish itself in some legal frameworks as a *sui generis* right, parallel to the right to privacy.

---


4 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28/1/1981 (Convention N° 108), and Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8/12/2001.


Automated processing of personal data is not, however, the only technological development which has triggered a need to come up with new or updated legal notions in the name of the right to respect for private life. And not all of such new mechanisms came to life through the prism of personal data protection. One of these mechanisms, unrelated to the processing of personal data, is the regulation of so-called unsolicited communications.

2 The Regulation of Unsolicited Communications

The European Union (EU) has been dealing with unsolicited communications and related practices for more than a decade. A chronology of this phenomenon could take 1997 as a starting point, and in particular the Directive 97/7/EC on the protection of consumers in respect to distance contracts. With explicitly reference to Article 8 of the ECHR, Directive 97/7/EC considered that the right to privacy of the consumer should be recognised, particularly as regards certain particularly intrusive means of communication. Thus, it established several restrictions on the use of certain means of distance communication, and, concretely, it required the prior consent of the consumer for the use of automated calling systems without human intervention and fax as a means of distance communication for the conclusion of a contract between the consumer and the supplier.

on its very content and on the content of the right to privacy, is still to be fully assessed. Such an assessment would in particular need to take into account the complexity of the EU system for the protection of fundamental rights, in which different levels of protection (the Council of Europe, the EU and the national legal frameworks) coexist and influence each other.

For example, the judiciary and the legislator were forced to rethink how to ensure the confidentiality of communications with the advent of the telephone, with the European Court of Human Rights eventually taking the view that the numbers dialled are an integral element in the communications made by telephone (Malone v. The United Kingdom, № 8691/79, European Court of Human Rights, 2 August 1984, Series A № 95, § 84) and consequently inspiring regulation from this perspective.


Recital (17) of Directive 97/7/EC.

Art. 10(1) of Directive 97/7/EC.
Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, also of 1997, contained equivalent provisions to be applied to unsolicited calls and faxes. With the aim of providing safeguards for all subscribers of telecommunication services against intrusion into their privacy by means of unsolicited calls and faxes, Article 12 established an opt-in regime for the use of any automated calling machines without human intervention, including faxes, for purposes of direct marketing.

Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) of 2000 was the first Directive to explicitly refer to a now very common type of unsolicited communications: electronic mail (‘spam’). Observing that the sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks, Directive 2000/31/EC introduced specific provisions to protect users from unsolicited commercial communications by electronic mail.

Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, deals in detail with unsolicited communications. Its Recital 40 reasons that safeguards must be provided for individuals against intrusion of their privacy by unsolicited communications for direct marketing purposes, in particular by means of automated calling machines, faxes, and e-mails, including SMS messages. This is so, it is clarified, because these forms of unsolicited commercial communications are relatively easy and cheap to send, and may impose a burden or cost on the recipient. Consequently...

13 Recital (22) of Directive 97/66/EC.
16 Recital (30) of Directive 2000/31/EC.
17 Art. 7 of Directive 2000/31/EC.
sequently, Article 13 of the Directive establishes that the use of automated calling systems without human intervention, of faxes or of electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent (‘opt-in’).20

Overall, these different provisions seem to respond to two common concerns deserving particular attention. First, they are based on the careful observation of constant technological and marketing developments, and have no vocation of technological neutrality: whatsoever. Their evolution proves that special care has been taken to keep continuously updating them, for instance by clarifying that their scope of application covers the latest advances of the time, be it faxes, electronic mails, or SMS messages. Second, the interest protected by the regulation of unsolicited communications is definitely a notion of ‘privacy’ unlinked to the protection of personal data.22 What is at stake are not the conditions related to the

20 Directive 2002/58/EC, Art. 13(1). Notwithstanding this general rule, Art. 13(2) established that where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same person may use these details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use. It shall be noted that, although Art. 13 aims at harmonising the conditions under which electronic communications can be used for marketing purposes, there is a general understanding that some of the concepts it uses appear to be subject to differences of interpretation in EU Member States (Article 29 Data Protection Working Party (2004). Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC. WP 90. Brussels, 27 February, p. 2).


22 This should not be interpreted as implying that other provisions contained in the Directives dealing with the regulation of unsolicited communications are not designed to develop the protection of personal data. Directive 2002/58/EC, for instance, is indeed partially concerned with ‘particularising’ the protection granted by Directive 95/46/EC (see Art. 1(2) of Directive 2002/58/EC: “The pro-
possible processing of personal data required to perform the communication, but a
much broader privacy-interest to which the unsolicited communication is in any
case felt to constitute an undesired intrusion or interference.

But how can this ‘privacy-interest’, protected by this mechanism, be conceptu-
ally framed? Directive 97/7/EC alludes to the right to privacy of the consumer;
Directive 97/66/EC mentions the privacy of the subscriber; Directive 2000/31/EC
aspires to broadly protect the user; Directive 2002/58/EC refers extensively to the
privacy of individuals.23 The nature of these provisions allow to envision such a
privacy as an interference-free space to which individuals are entitled to, and to
which they should not be obliged to renounce even if they choose to subscribe to a
telecommunications network, or to use information society services. In this sense,
the regulation of unsolicited communications is not concerned with persevering a
private space from all external interferences, but more precisely with safeguarding
the possibility of enjoying such space needed for the building up of our person-
ality, by limiting unrequested and undesired interferences. From this point of
view, autonomy (rather than seclusion) lies at the core of the legislator’s privacy
concerns.24

It this perspective, the mechanism can be related to a more global, and possibly
currently emerging right of privacy of the consumer, or right of the consumer to be (relatively) left alone25 and to be protected against unwanted and unasked at-

visions of this Directive particularise and complement Directive 95/46/EC for the
purposes mentioned in paragraph 1”).

23 Even though it is not exclusively concerned with the protection of natural
persons, but also with the protection of legal persons (see, notably, Recitals
(12) and (45) and Art. 1(2) of Directive 2002/58/EC).

24 Thus demonstrating the relevance of relying on a notion of privacy as a
concept serving a multiplicity of values (see note 2). See also: Rouvroy, A. and
of Self-Development: Reassessing the Importance of Privacy for Democracy. In
Gutwirth, S., Y. Poullet, P. De Hert, C. de Terwangne (Eds.), Reinventing data
protection?, Dordrecht: Springer Science, 45-76.

del consumidor: a no ser molestado y a una interacción informativa. Revista gene-
ral de legislación y jurisprudencia, 2, 175-193. The connections between con-
sumer law and privacy protection have been increasingly explored during the past
years, especially as privacy has been positioned as a key element of consumer
aspects juridiques des systèmes d’information. Lex Electronica, 10(3), available at
http://www.lex-electronica.org/articles/v10-3/poullet.htm, p. 15; Alleweldt, F.,
Briefing Note, European Parliament, PE382.173, p. 11), but much more could be
tempts to influence and steer the consumer’s behaviour. This right is believed to inspire not only the regulation of unsolicited communications, but also the establishment of minimum rules and standards on television advertising, for instance as established already in 1989 by the Directive 89/552/EC on the coordination of certain provisions concerning the pursuit of television broadcasting activities.26 Directive 89/552/EC stated that such rules and standards were essential in order to ensure that the interests of consumers as television viewers are fully and properly protected,27 and similar provisions were later to be found in Directive 97/36/EC, of 1997,28 or in the 2007 ‘Audiovisual Media Services Directive’29. The rationale behind this type of provisions is that, although advertising might have its advantages, it needs to be regulated so it does not have a detrimental effect on the enjoyment of television by its viewers.30 Certainly be done to reinforce them, in particular by reinforcing the effectiveness of privacy protection through consumer law mechanisms. 


27 See Art. 11 of Directive 89/552/EEC.


30 The intention here is thus not to preserve the privacy of individuals against the risks of television consumption, but to make sure that individuals can access television programmes without suffering the burden of excessive advertising. For an understanding of television as a force marking the destruction of privacy by taking individuals away from their private intensions, see: Wright Mills, C. (1956, 2000. The Power Elite. New York: Oxford University Press, p. 314.
3 The Shift Towards Unsolicited Adjustments

If the interest protected by the regulation of unsolicited communications is still to be effectively preserved in the future, it is crucial to keep adequately updating it. This is true not only because technical developments are continuously taking place, and unsolicited communications come regularly in new forms and shapes, but also because marketing practices are evolving. The evolution does not affect solely the technical nature of communications. It is more radical and profound. To better grasp its proportions, we should consider both current presaging practices and progress expected in the long term. We will start with the latter.

3.1 Upcoming Practices

Prospective developments in this area are delineated by the upcoming ‘ubiquitous computing’ and ‘ambient intelligence’ scenarios. This is a future in which objects are interconnected and communicate with each other, while also being able to interact with individuals. This is a future in which the on-line world meets the off-line world, and everything potentially reaches the on-line status. Devices, embedded in the environment and furnished with sensors, are context-aware; they react to changes by adapting their behaviour, and are even able to anticipate them. This is the time of ‘smart’ homes, in which ‘smart’ kitchens are equipped with ‘smart’ freezers keeping track of daily consumption to timely suggest purchasing milk before it goes off, or are even programmed to automatically order it from a selected store.

According to the examples put forward by companies investing in this field, ‘smart’ objects would seem to respond to some sort of neutral, almost philanthropic interests, always advising what is genuinely the best for the individual based on factual information virtuously collected and some mysteriously unprejudiced guidance. Nevertheless, there is no reason why this should occur entirely this way. If the on-line world is really going to meet the off-line world, online marketing practices, and, in particular, online behavioural advertising are not to disappear, but to turn pervasive. Marketing practices based on predictive data mining and consumer profiling, now pullingulate on the Internet, are to be rolled out.

through the ‘smart’ freezers, in our private (‘smart’) kitchens, across our private (‘smart’) homes.

It appears extremely difficult to determine what should be considered as an ‘unsolicited communication’ in this kind of context. Actually, it is already highly laborious to decide what should be designated in these future scenarios as a ‘communication’, as most of the messages conveyed from object to object, and even from objects to individuals, would fail to qualify as communications in a traditional, legal sense. Might a ‘smart’ freezer announcing on its door that there is no milk left inside, be considered as a communication? Would it be doing so if it simultaneously sent an SMS to the householder? What about if every time the door is opened and there is almost no milk left, a jingle informs about discount prices on milk at a nearby store? What if the freezer suddenly offers the possibility to directly purchase more milk from a new, unknown but ‘recommended’ brand by simply touching an icon? And if all these practices are not really communications, what are they? Are they simple functionalities of the object, just like any other? Are they decisions the freezer ‘smartly’ takes on its own?

Linguists have been discussing for decades about the thin line separating mere statements, which purely inform, to performative utterances, which do not only comment about reality, but change reality. They eventually even questioned whether such a thin line existed at all, as in a sense all utterances have an impact on reality. Marketing practices in upcoming ‘ubiquitous computing’ and ‘ambient intelligence’ scenarios might be better understood by acknowledging that the key issue with them is not whether they constitute a mere communication, an actual decision, or an adaptation facilitating a decision by the individual. What should be clear is that a series of practices, not restricted to our current idea of what a ‘communication’ is, can constitute invasive practices, just as unsolicited communications do now. They can be thus viewed as falling under a wider category of ‘adjustments’ or automatic adaptations of software or devices to be described as unsolicited adjustments, and deserving ad hoc regulation.

3.2 Present Problematic Practices

The discussion of future scenarios should not lead the reader to believe that this style of practices are not being developed and implemented right now. Some ap-

---

32 For instance, Directive 2002/58/EC defines ‘communication’ as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service” (Art. 2(d)).

Applications used in contemporary computers or ‘smart’ phones already tend to follow the same logic, by systematically privileging the direct adaptation of their behaviour, or features, instead of sending communications to the users to invite them to envisage such adaptations. It is the case, for instance, when devices seem to take the initiative to connect with a specific service, to download a particular file or software, or to re-tailor the user’s preferences. But we should now consider another type of example, apparently very distant but ultimately fully pertinent.

This example takes us outside the private space of the home, to the indubitably public space of public transport. More concretely, it takes us to the Parisian metro, where the deployment of a new type of digital interactive advertisement screens caused much controversy, and notable indignation by the civil society, in the spring of 2009. The digital screens, to be installed in the corridors of the Paris underground, were labelled as ‘spying’ monitors: looking like simple screens, they actually hid two cameras and an electronic system allowing to count the number of persons passing by, to measure for how long they looked at the screen and to analyse their reactions in order to detect which element of the image had caught their attention. The system was also capable, in principle, to provide information about the age and gender of people walking by.

All the screens were equipped with Bluetooth technology, and the company responsible for them had originally planned to allow for the sending of messages via Bluetooth to the mobile phones of all passers-by. This idea, however, was strongly opposed by the French authority responsible for the monitoring of compliance with privacy and data protection legislation. In the name of the regulation of unsolicited communications, the authority considered that the practice would be unlawful, as the consent of the subscriber was needed before the communication was sent, and without such prior consent no communication for marketing purposes was possible. The Bluetooth functionality was eventually deactivated.

It soon appeared that there was little more that the French authority could do in this case, and its reaction might be considered illustrative of some hesitations

---

34 Five French NGOs (Résistance à l’agression publicitaire, Souriez vous êtes filmés, Big Brother Awards, Robin des toits and Le Publiphobe) introduced a complaint against the companies responsible for the advertisement in the Parisian underground because of the mentioned screens. For the official press release dated from April 22, 2009 see: http://bigbrotherawards.eu.org/Ecrans-de-pub-interactifs-la-RATP-et.html.

35 Called Majority Report.

36 Commission nationale de l’informatique et des libertés (CNIL).

and inadequacies of the existing legal framework for privacy protection in Europe. Facing an operative screen already in place, the authority assessed that the device in question was simply measuring the screens’ audience, by measuring the number of passers-by looking at it and for how long they did so. As the images were not recorded, transmitted or visible to anybody, it concluded that provisions related to CCTV were not applicable. The authority argued, nevertheless, that the screens might be viewed as personal data processing equipments, because, although they stored only the mentioned statistical information, in order to obtain it they were processing images that included identifiable faces, to be qualified as personal data, thus triggering the applicability of data protection provisions. If this argument were considered valid, then the screens would have to comply with data protection legislation. However, it would suffice to the company to claim that the faces were blurred and not related to identifiable persons not to have to comply with any data protection legislation, and it is clear that the company has no particular interest in identifying anybody, as identifying the passers-by does not provide any added value. The weakness of the protection offered is consequently obvious.

This weakness becomes much more worrying when we take into account all the functions that this type of advertisement screens are in principle designed to perform. Another company active in the same market, for instance, offers very similar performances but promises to announcers using its so-called ‘dynamic advertisement networks’ real time information on the number of viewers attracted, the exact distance they were at, and their demographic profile. If the demographic profile is obtained in real time, the next logical step for any announcer should be to adapt the content of the advertisement showed on the monitor taking into account such information, also in real time, for enhanced targeting. If tempted to do so, current provisions on unsolicited communications would not be an obstacle, as they would not apply to this kind of advertising. It certainly can appear to be totally inconsistent to pretend, on the one hand, that because of privacy protection announcers cannot send messages via Bluetooth to the mobile phones of passers-by even if they are walking around by their Bluetooth device knowingly activated. But also allow, on the other hand, the same announcers to freely and systemati-

92 92

92
cally scrutinize all passers-by without their knowledge, to try to guess their age and gender and, that based on this information, to furtively adapt the content of

38 And as the actual determination of the age and gender of audience was not being operated in that particular case.
39 Closed-circuit television.
40 Named Quividi.
41 See: http://www.quividi.com/fr/message_targeting.html
their advertisements, and force passers-by to endure all this process and the resulting adapted advertisement even if they just want to use the public transport and are not even carrying on any electronic device at all. Unfortunately, the existing regulation dealing with unsolicited communications backs up this kind of paradoxical outcome.

### 3.3 The (other) Limits of Current Legislation

One might think that, despite the limitations of the present regulation of unsolicited communications, other legal mechanisms are already in place to effectively guarantee the right to respect for private life of individuals in front of the described developments. This is not exactly the case. The deficiencies of personal data protection in these situations have already been coined. Provisions on personal data protection do not apply when personal data is not processed, and there is actually no need to process data obviously falling under the traditional notion of ‘personal data’ to perform a communication or adjustment constituting an intrusion of the privacy of the individual. This configures the greatest weakness of traditional data protection in this field.

Online behavioural advertising is already highlighting this crucial flaw of data protection, and unsurprisingly much of the legal discussion surrounding the issue

---


43 Defined as “any information relating to an identified or identifiable natural person (‘data subject’)” in Directive 95/46/EC (Art. 2(a)).

44 These observations are not meant to suggest that the current problems faced by personal data protection law are insurmountable. Many efforts have been deployed to refine and reinforce data protection law, and they should certainly be backed up.

45 For the moment, regulated mainly through self-regulation efforts. See, for instance: International Advertising Bureau (IAB) (2009). Good Practice Principles for Online Behavioural Advertising; Federal Trade Commission (2009). FTC Report: Self-Regulatory Principles for Online Behavioral Advertising, February. Online behavioural advertising practices can also be instructive from the perspective of the regulation of unsolicited adjustments because of the innovative and sometimes subtle ways in which marketing practices sometimes take place, for instance by embedding product endorsements or blurring distinctions between
has focused on whether the data used is personal data or not. Online behavioural advertising relies on the processing of user-specific data collected while monitoring the on-line conduct of individuals, but companies executing it will tend to contest that this data relates to identified or identifiable persons, thus maintaining that data protection provisions are not applicable. As a response to such a strategy, and as far as online behavioural advertising is concerned, there is still the possibility to argue that the practice also affects another mechanism of privacy protection, which is unrelated to personal data: the right to confidentiality of communications. Indeed, online behavioural advertising will generally be undertaken intercepting, monitoring and even altering communications that, in the name of the right to confidentiality of communications, might deserve to be kept free from any interference.

This argument, however, would not apply when behavioural advertising is no longer deployed on-line, but off-line, and when the conduct monitored does not consist of any communication activities but relates, for instance, to milk consumption in the private space of the home. In that case, it is true, we could try to invoke still another mechanism for privacy protection, which is the protection of the home. But that mechanism would no longer be applicable when we consider the example of the ‘spying’ screens in the corridors of the underground.

A last relevant possibility is, when unsolicited adjustments are based on profiling, the regulation of automated decision-making. Existing regulation, nonetheless, would not guarantee any effective protection, as provisions are generally concerned with decisions that per se produce legal effects or significantly affect individuals, which would not be the case with the majority of unsolicited adjustments. Altogether, it appears that at the moment no concrete legal tool ensures effectively the interests of the individual in front of the described developments.

4 Concluding Remarks

This contribution has argued in favour of widening the protection currently granted through the regulation of unsolicited communications via the new notion of ‘unsolicited adjustments’. We have shown that the evolving nature of communications and, more generally, of marketing practices, urgently requires a rethinking of the existing legal mechanisms. Otherwise, current developments will

---


46 Such as Art. 15 of Directive 95/46/EC.
continue to benefit from the existing legal loopholes and, slowly but surely, tend to design a world in which objects that are supposedly there in order to assist and guide, in practice secretly track individuals, to surreptitiously adapt their performances based on undisclosed criteria.

In our description of unsolicited communications, we have highlighted that the interest protected by their regulation and related provisions appears to be the privacy of the individual, sometimes envisaged as a 'consumer', as a ‘subscriber’ or as a 'user'. Although such privacy of the individual is never described or defined, its preservation is envisaged as an aspect of the right to respect for private life. Thereby, the mechanism ultimately serves the very same goals pursued by Article 8 of the ECHR, which are certainly not limited to the mere insurance of a sheltered space in which individuals can (relatively) peacefully watch television, receive solicited phone calls or electronically purchase products just for the sake of it. Fundamentally, the mechanism is intended to guarantee such privacy of the consumer, of the subscriber, of the user and, in general, of the individual or citizen as an instrument favouring self-development and personal autonomy, and ultimately, as all privacy-related legal tools, his or her freedom.

5 References list


This approach would be fully consistent with Sunstein’s very important analysis of the possible negative impact on citizenship of excessive consumer choice (Sunstein, Cass R. (2007). Republic.com 2.0. Princeton, PA: Princeton University Press, p. 136). Unregulated unsolicited adjustments would not serve consumer choice, but could, on the contrary, tend to eradicate it by replacing it by the absolute impossibility of the choice for consumers, and the imposition on them of a certain vision of reality, predetermined by third parties. This imposition could have the same negative impact on citizenship as excessive consumer choice, or, possibly, even worse effects. Only by preserving the possibility for individuals to be released from these practices and confronted with the unexpected and the presumably unwanted can their ability to chose be ensured.


