Confidentiality and the (Un)Sustainable Development of the Internet

Marcello D'Ambrosio∗

Abstract

The right to privacy is compromised on a daily basis by the commercial practices of today’s information society. The Schrems case is an example of the risks of the processing of personal data on the internet. The European regulatory system for the protection of personal data cannot ensure effective protection of its citizens’ information. Therefore, this article proposes a reconceptualisation of the internet by classifying it as an aspect of the environment in which people live. Although it is a virtual dimension, there is still a need to apply the rules established to protect the real habitat, such as, for example, those that recognise a specific corporate social responsibility.

I. Introduction: Lost Privacy

There was once a young student who had long conversations, posted images of his life and opinions of all kinds via a large virtual community of friends, like all of his peers. In short, thanks to the community, he was in contact with others, and his life was shared with them.

As in the best stories, it is worth including an element of drama, in this case, Orwellian.

One day, the hero of our story found out that all of this information, which he had given in good faith to the community, was transferred and collected in another country, far from his own. Upon hearing the news, he was amazed, as he had never thought about where all of the different aspects of his private life were preserved. Unfortunately, that was not all. The young man learned that the information was at the mercy of the State where the community had sent it. The intimacy of his life had been violated. He was not as safe as he had believed.

The student therefore decided to seek justice. He appealed to a judge, who received his complaints, recognised the injustice of what had happened, and in order to protect the young man, eliminated the conditions which led to the violation of his rights and his freedom.

∗ Assistant Professor of Private Law (tenured) (PhD), University of Salerno, School of Economics and Statistics.
It could be possible to conclude that they lived happily ever after! However, what seems like a happy ending actually is not.

Narrative prudence would include a warning that any reference to real events or circumstances is totally random. However, this story is not fictional, but a recounting of real events. The protagonist of the story is, in fact, Maximilian Schrems, an Austrian student, who one day decided to challenge the opaque personal information management practices of the most famous global social network.

In order to address the challenges posed by the (un)sustainable development of the internet, the present essay is structured as follows: part II describes the Schrems case; part III discusses the current regulatory environment as regards protection of privacy; part IV highlights the environmental dimension of the internet and the role of market participants in leading its development; and finally, part V focuses on Corporate Social Responsibility as potentially a feasible way to address the issues at stake.

II. The Schrems Case

The Schrems case, decided by the European Court of Justice on 6 October 2015, is one of the recent cases that have been among the most shocking to the internet community.

Judges in Italy and around the world often make decisions regarding

---


3 In relation to foreign courts, for example, in Germany see Bundesgerichtshof 14 May 2013, with commentary by G. Giannone Codiglione, ‘Funzione “auto-complete” e neutralità del prestatore di servizi’ Diritto dell’informazione e dell’informatica, 541-557, 547 (2013); and Eur. Court H.R., Delfi AS v Gov. Estonia, Judgment of 10 October 2013, with commentary by F. Vecchio, ‘Libertà di espressione e diritto all’onore in Internet secondo la sentenza “Delfi As contro Estonia” della corte europea dei diritti dell’uomo Diritto dell’informazione e...
the internet. It is worth considering the cases related to the liability of hosting providers, which consider the recognition and protection of the so-called right to be forgotten.⁴ However, service providers have generally failed to implement the guidelines created by these cases. Although some judges have attempted to challenge the service providers’ responsibility regimes, which strongly favour their own interests,⁵ significant breaches in the security systems of information society companies have appeared.⁶

⁴ Recently, Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos (European Court of Justice Grand Chamber 13 May 2014) available at www.curia.europa.eu. European judges recognise in the holder of personal data, the object of treatment, the right to control over the protection of their own social image, which can result, even in the case of real news, for the record, in the claim to the ‘contextualisation and updating’ of the same, and if appropriate, also to its deletion. This is because the owner of an online information organisation is recognised as responsible for ensuring the constant updating of disclosed information. The fact that this information is moved, after some time, to historical archives published on the web, does not exempt the internet site operator from the obligation of maintaining ‘the characters of truth and accuracy and therefore of lawfulness and fairness, the right to protection concerned the treatment of the moral or personal identity as well as safeguarding of the citizen’s right to receive complete and correct information’. More recently, on a national level, Tribunale di Roma 3 December 2015, Foro Italiano, I, 1040-1044 (2016). See the particular position of the Tribunal de grande instance de Paris 24 November 2014, Diritto dell’informazione e dell’informatica, 532-538 (2015).


⁶ See Tribunale di Milano 12 April 2010 n 2 above, 2232; and Tribunale di Milano 31 March 2011, with commentary by E. Tosi, ‘La responsabilità civile per fatto illecito degli
In contrast to these cases, the Schrems case immediately assumed – and continues to have – extraordinary economic and diplomatic importance.

At this point, it is necessary to retell the story.

The Schrems case called on the Court of Justice to interpret Arts 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and Arts 25, para 6, and 28 of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data – in this case, making reference to the provisions governing the transfer of data to third countries and the establishment of supervisory authorities in relation to data processing. In addition, the Court of Justice was requested to rule on the validity of Decision no 520 of 2000 of the European Commission (the so-called Safe Harbour), and in particular, on the adequacy of the protection offered by the principles contained therein and the information on privacy published by the Department of Commerce of the United States of America.

The appeal arose in the context of a dispute between Schrems and the Irish Data Protection Commissioner concerning the Commissioner’s refusal to investigate a complaint filed by Schrems about the fact that Facebook Ireland transfers the personal data of its users to the United States, storing it on servers there.

Schrems requested the Commissioner to exercise his powers to prohibit the transfer of personal data, based on the assertion that the law and current practices in the United States did not offer sufficient protection of personal data against control activities by public authorities. Schrems was referring to revelations made in 2013 by Edward Snowden, a former CIA technician, regarding mass-media surveillance programs set up by US intelligence, in particular the National Security Agency (NSA).

The Irish Commissioner dismissed Schrems’s complaint as unfounded on the basis of the absence of evidence that the NSA had had access to the personal data concerned. The Commissioner also added that the complaints put forward could not be invoked, since the level of protection of personal Internet service provider e dei motori di ricerca a margine dei recenti casi “Google suggest” per errata programmazione del software di ricerca e “Yahoo! Italia” per link illecito in violazione dei diritti di proprietà intellettuale’ Rivista di diritto industriale, II, 17-66, 44 (2012).

For further details, see http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000D0520 (last visited 6 December 2016).

For further details, see www.export.gov/safeharbor/index.asp (last visited 6 December 2016).

data in the United States had been assessed by the Commission to be in compliance with European law through the so-called Safe Harbour.

Subsequently, Schrems appealed the decision of the Commissioner before the Irish High Court, which held that although the electronic surveillance and interception of personal data transferred from the European Union to the United States was necessary for the public interest, Mr. Snowden’s revelations showed that the NSA and other federal agencies had committed ‘considerable excesses’.10

The Court of Appeal found that the matter concerned the implementation of EU law under Art. 51 of the Charter of Fundamental Rights, so that the legality of the decision referred to in the main proceedings had to be assessed on the basis of EU law. According to the Irish judges, the Safe Harbour did not meet the requirements of European law. For the High Court, the right to respect for privacy,11 as guaranteed by the Charter of Fundamental Rights and the constitutional systems of many Member States,12 would be meaningless if the authorities were authorised to access electronic communications on a random and generalised basis, without any objective justification based on the grounds of national security or crime prevention.

Based on this interpretation, the Irish High Court suspended the proceedings and referred the case to the Court of Justice for a preliminary ruling. The Irish judges asked the European Court of Justice whether and to what extent, in light of the Charter of Fundamental Rights, Directive 95/46/EC should be interpreted as meaning that a decision adopted under that Directive (such as the Safe Harbour) prevents a national supervisory authority from examining the application of a party requesting protection for personal data transferred to a third country whose legal system does not ensure an adequate level of protection.

10 High Court of Ireland 18 June 2014, available at http://www.courts.ie/Judgments.nsf/0/481F4670D038F43380257CFB0044BB125 (last visited 6 December 2016), wherein it is also recognised that ‘(g)iven the general novelty and practical importance of these issues which have considerable practical implications for all 28 Member States of the European Union, it is appropriate that this question should be determined by the Court of Justice’.

11 Ibid: ‘in this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home – such as e-mails, text messages, internet usage and telephone calls – would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation’. On top of that, the controversial effectiveness of the Safe Harbour principles was called into question by the Commission itself in 2013 and fuelled new negotiations between the EU and the US. To this extent, see X. Tracol, ""Invalidator" Strikes Back: The Harbour Has Never Been Safe’ 32 Computer Law and Security Review, 345, 348-349 (2016); and M. Corley, 'The Need for an International Convention on Data Privacy: Taking a Cue from the CISG’ 41 Brooklyn Journal of International Law, 721, 750 (2016).

12 Arts 7 and 8 of the Charter of Fundamental Rights of the European Union, and, for example, Arts 13-15 of the Italian Constitution.
This requires examination of the meaning of an ‘adequate level of protection’. The Court of Justice stated that although it cannot ‘demand that a third country ensures a level of protection identical to that provided by European Law’, the expression ‘adequate protection’ must be interpreted so as to mean that the third country must ensure ‘effectively, in view of its national legislation or its international commitments, a level of protection of freedom and fundamental rights substantially equivalent to that provided in the European Union’. The Court stressed that otherwise ‘the high level of protection guaranteed by European law could be easily circumvented by transfers of personal data (...) to third countries’. This point illustrates a common fear that partially recurs in the present case.

Essentially, the European judges allowed that the instruments that a third country uses to ensure an adequate level of protection might be different from those implemented in the EU. However, in order to ensure compliance with the requirements of European legislation, these instruments must nevertheless ‘be effective in practice, in order to ensure a substantially equivalent protection’ throughout Europe.

Thus, the interpretation offered by the Court of Justice implies a strict standard and raises some concerns.

Initially, the European judges held that a provision allowing public authorities to gain general access to the content of electronic communications ‘undermines the essential content of the fundamental right to privacy’. For the Court, a valid decision, such as the one regarding the Safe Harbour, requires a finding that the third country in question effectively ensures a level of protection of fundamental rights equivalent to that provided under European law.

Since the Commission, in the Safe Harbour decision, did not ‘claim’ that the United States effectively ‘guarantees’ an adequate level of protection, the Court did not find it necessary to ‘examine the Safe Harbour Principles in terms of their content’, but rather concluded that the Commission’s decision infringes the requirements set out by European legislation and is, for this reason, invalid.

Thus, the Safe Harbour has been eliminated, as it was found to be too vague and too lenient regarding the transfer and processing of personal data.
in (or directed towards) the United States. The effects of this ruling are still unfolding. If the Safe Harbour agreement falls short, there is no longer a guarantee that the transfer and processing of personal data in (or directed towards) the United States is compliant with an adequate level of protection. Nevertheless, mutatis mutandis, some might say: The undertaking must go on! The ball seems to have been passed to the national supervisory authorities, which have the power to examine individual instances of the protection of privacy in relation to information that has been transferred from the EU to a third country.

III. Protection of Privacy

The issue of protection of personal data is part of a delicate institutional relationship. In October 2015, the Italian Data Protection Authority, in light of the ruling in the Schrems case, issued a measure (no 564) entitled ‘Personal data transfer to the US: unconstitutionality of the Authority ruling of 10 October 2001 of recognition of the agreement on the so-called ‘Safe Harbour’’. With this measure, the Guarantor for privacy nullified a previous authorisation that allowed the transfer of data to the United States and made clear that in order to transfer information overseas, multinational companies, organisations and Italian companies will have to make use of other possibilities provided for by the legislation on the protection of personal data.

The Guarantor therefore confirmed that the businesses can lawfully transfer the data, but only by making use of tools such as model contracts or Codes of Conduct adopted within the same group (the so-called BCR, Binding Corporate Rules). The Control Authority has ultimately retained the power to verify the legality and correctness of the data transfer from those who export them.

In the absence of an agreement, the trans-border transfer should be allowed in light of the exceptions laid down by Art 26 of Directive 95/46/EC and the Data Protection Code. The reference, in this case, is to the authorisation freely expressed by the parties concerned on the basis of a

---

21 The Authority, in this way, ‘orders the unconstitutionality of the authorisation adopted by the Authority on 10 October 2001 by resolution n. 36 and the effect prohibits, under Arts 154, paragraph 1, lett. d) and 45 of the Code, to the exporters subject to transfer, on the basis of this resolution and of the conditions specified in that, personal data from the State’s territory to the United States of America’.
22 Arts 43 and 44 Data Protection Code.
specific and informed consent, through the use of model contracts.\textsuperscript{23}

The Control Authority emphasised that these contractual provisions must, however, be quoted or incorporated into contracts so that they can be recognisable to the people to whom the data refers to, or to those who ask to access it.\textsuperscript{24}

Returning to the specific issue in the Schrems case, the transfer of data by Facebook Ireland to the United States seems to have reached a questionable impasse. The Court of Justice chose to privilege the protection of privacy over business activities, thus forcing European and North American institutions to promptly counterbalance the potentially negative economic consequences of the ruling.\textsuperscript{25}

In February 2016, the EU and the United States took an important step to overcome the dispute by reaching a new agreement to replace the Safe Harbour. The Privacy Shield\textsuperscript{26} is a new international agreement that aims to

---

\textsuperscript{23} Which gives authorisations, ex art 44, para 1, letter b) of the Data Protection Code, by the Guarantor dated October 10, 2001, by resolution no 35 (doc web no 42156), 9 June 2005, by resolution no 12 (doc web no 1214121) and 27 May 2010, by resolution no 35 (doc web no 1,728,496, in this regard, see also the subsequent Authority Provision of 15 November 2012, web doc no 2191156); or otherwise by reason of the adoption, within companies belonging to the same group, the rules of conduct in Art 44, para 1, letter a) of the Data Protection Code, referred to as Binding Corporate Rules (‘BCR’, cf in order to ‘Bcr for Controller’ among others, the documents of the ‘Group ex Art 29’, WP 74 of 3 June 2003, WP 108 of 14 April 2005 and WP 153 of 24 June 2008; whereas, with regard to ‘Bcr for Processor’, the documents WP 195 of 6 June 2012 and WP 204 of 19 April 2013); or if they are authorised by the Guarantor, pursuant to Art 44, para 1, letter a) of the Code, on the basis of appropriate safeguards for the rights identified by this scheme in relation to warranties offered with a contract. For the definition of the Model Contracts for the transfer of personal data to third countries, see http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited 6 December 2016).

\textsuperscript{24} Ruling by the Authority for Personal Data Protection no 35 of 10 October 2001 (doc web no 42156), available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1669728 (last visited 6 December 2016), with it being set out that ‘the data exporter and the data importer refer to or incorporate the clauses in the data transfer contract so as to make them also recognisable for the individuals to whom the data refer, where they request to be informed about the clauses; additionally, they may not lay down contractual provisions that impose limitations on or contradict the standard contractual clauses (see Clause no 4, letter c) and no 5, letter e), and Recital no 5 in the Commission’s decision’.


re-establish confidence in the flow of data by providing a system of rules with which US companies are required to comply when handling the data of European citizens.

In addition, the US government formally committed itself to ensuring the implementation of the agreement. The goal is to prevent the US authorities from gaining general access to European citizens’ data in the future. In this sense, US companies will have to comply with solid obligations concerning personal data processing to guarantee the rights of individuals, while the Department of Commerce of the United States will have to verify that the companies publicly disclose their commitments.27

Nevertheless, in September 2016, Facebook’s website on ‘data-regulation’ in the ‘how our global services operate’ section still reads:

‘Facebook Inc. complies with the Safe Harbour framework, in force between the US and European Union (…), in relation to the collection, use and retention of data from the EU. Information collected within the European Economic Area (‘EEA’) may be transferred to countries outside for the purposes described in this policy’.28

Currently, Facebook only refers to the standard contractual clauses approved by the European Commission. However it is not clear to the user where to find these clauses and when they have been signed. Facebook has no other relevant provisions in its contract or in its declaration of rights and responsibilities. Therefore, a transfer of data by Facebook to the United States would not be adequately safeguarded in accordance with Art 25 of Directive 95/46/EC and Arts 43 and 44 of the Data Protection Code.

It is therefore ironic that the service provider has continued for many months to refer to an agreement that is no longer valid. Above all, it is surprising to note that there are no clear and recognisable contract clauses allowing for an agreement to weaker personal data protection legislation. The transfer to the North American servers would thus seem to take place outside of a fully legal context.29


See https://www.facebook.com/privacy/explanation# (last visited 6 December 2016).

The Data Protection Commissioner has announced, through the document ‘Statement by the Office of the Data Protection Commissioner in respect of application for Declaratory Relief in the Irish High Court and Referral to the CJEU’ that ‘We continue to thoroughly and diligently investigate Mr Schrems’ complaint to ensure the adequate protection of personal data. We yesterday informed Mr Schrems and Facebook of our intention to seek declaratory relief in the Irish High Court and a referral to the CJEU to determine the legal status of data transfers under Standard Contractual Clauses. We will update all relevant parties as our
Alarmingly, this phenomenon involves more than thirty five million users in Italy alone. What is even more noteworthy is the position of the Guarantor for the protection of personal data, who, as previously mentioned, formally verifies the legality and correctness of such data transfers: he does not seem to have taken a position on this particular case, and is probably waiting for a user complaint.

IV. The Internet as an Environmental Dimension

The Schrems case is only one of numerous disputes highlighting a need to reconsider the internet as neither as a mere communication tool nor as a simple market space. It is necessary to be fully aware of the relationship between the internet and the habitat in which individuals live.

According to a common definition, the environment is everything that surrounds an organism. It refers to a complex system that surrounds a subjective reference point. This leads us to think that this universe of elements investigation continues’, available at https://www.dataprotection.ie/docs/25-05-2016-State-
ment-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-
and-Referral-to-theCJEU/1570.htm (last visited 6 December 2016).

The data are taken from http://www.panorama.it/mytech/social/facebook-numeri-
impressionanti/ (last visited 6 December 2016).


See the item ‘Ambiente’ available at www.treccani.it.
has an exclusively physical nature. The environment is imagined as a natural place made up of biotic and abiotic elements in which individuals are immersed. However, it is worth noting that, for some time, many other factors contribute to the definition of environment. This is evident when considering the current parameters used to define the quality of a habitat in which people live. A healthy environment, in fact, no longer depends only on the natural characteristics of places, but also on the social aspects, which mirror the relationships between individuals. The reference is to intangible, non-physical characteristics, which are deeply relevant in determining the quality of life of people.

Individuals in the globalised world are immersed in a context that is no longer exclusively related to their place of birth or residence. People constantly operate in a virtual space, where they establish both economic and personal relationships, while considering the internet to be their future. The internet expresses human nature, and thus, is a metaphysical extension of the environment in which humans live and work.

This highlights the need for this dimension of the habitat to be governed by regulations that take into consideration the value of the person. Too often, rules are shaped to satisfy, first of all, economic interests. The regulatory framework of the internet consists of a set of rules that mostly regulate economic aspects. The early concern of European legislators, and in turn,
of national ones, was to contribute to a booming economic phenomenon and the significant potential for business development. The aim was to define a nurturing regulatory environment for financial transactions, and in general, private businesses. The objective of ensuring growth in the volume of
decreto legislativo 9 April 2003 no 70 on 'Implementation of Directive 2000/31/EC on certain legal aspects of information society services in the internal market, with particular reference to e-commerce'.

39 A set of limits are represented by L. Bugiolacchi, (Dis)orientamenti giurisprudenziali in tema di responsabilità degli internet provider (ovvero del dificile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito), commentary at Tribunale di Roma 16 December 2009, Responsabilità civile e previdenza, 1568-1599 (2010); and G. Pino, 'Assenza di un obbligo di sorveglianza a carico degli internet service providers sui contenuti immessi da terzi in rete' Danno e responsabilità, 832-840 (2004); G.M. Riccio, 'La responsabilità degli internet providers nel d.lgs. n. 70/2003 Danno e responsabilità, 1157-1169 (2003); R.H. Weber and S. Gunnarson, 'A Constitutional Solution for Internet Governance' 14 The Columbia Science & Technology Law Review, 1, 47-71 (2013); B.A. Oliver, n 5 above, 126-138 (2013); W.C. Larson, 'Internet Service Provider Liability: Imposing a Higher Duty of Care' 37 The Columbia Journal of Law and the Arts, 573-582 (2014); G.M. Martins and J.V. Rozatti Longhi, 'Internet Service Providers' Liability for Personal Damages on Social Networking Websites' 11 US-China Law Review, 286-309 (2014). However, the company cannot underestimate the impact of its activities in the social context. The doctrine has raised the issue that any economic activities should not adversely affect the environment in which they are carried out: see A. Berle, 'Corporate Powers as Powers in Trust' 44 Harvard Law Review, 1049 (1931); E.M. Dodd, 'For Whom Are Corporate Managers Trustees' 45 Harvard Law Review, 1148-1163 (1932); as well as the considerations expressed by K. Davis and R.L. Blomstrom, Business and Society: Environment and Responsibility (New York: McGraw-Hill, 1975), 50; by W.C. Frederick, From CSR to CSR: The Maturing of Business and Society Thought (Pittsburgh: University of Pittsburgh, 1978), 5. More recently, see M. Burri-Nenova, 'Trade Versus Culture in the Digital Environment: An Old Conflict in Need of a New Definition' 12 Journal of International Economic Law, 17, 34-45 (2009). This hermeneutic option has been called into question by both scholars and case law. As to the former, see M. Friedman, 'The Social Responsibility of Business is to Increase its Profits' The New York Times Magazine (1970), available at www.colorado.edu/studentgroups/libertarians/issues/friedman-soc-resp-business.html (last visited 6 December 2016); for a quick recap of the main terms of the debate, see L. Moratis, 'Out of the Ordinary? Appraising ISO 26000's CSR Definition' 58 International Journal of Law and Management, 26, 27-28 (2016). As to case law, see Tribunale di Roma 27 April 2016, available at www.phurisonline.it; contra Corte d'Appello di Milano 27 February 2013, Giurisprudenza italiana, 2633 (2013), it is therefore worth highlighting that there would be no obligation to prevent crimes committed by users for the heads of the host providers, even if active, 'since there is no legal provision that requires them to stop other people's offenses, nor the preventative powers competent to conduct such an activity effectively'. See V. Zeno-Zencovich, 'I rapporti tra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari)' Diritto dell'informazione e dell'informatica, 1049-1057, 1050 (1999); J. Bayer, 'Liability of Internet Service Providers for Third Party Content' 1 Victoria University of Wellington Working Papers Series, 1, 59-84 (2008); A. Anchayil and A. Mattamana, 'Intermediary Liability and Child Pornography: A Comparative Analysis' 5 Journal of International Law and Technology, 48, 55-57 (2010); K. Weckström, 'Liability for Trademark Infringement for Internet Service Providers' 16 Marquette Intellectual Property Law Review, 1, 30-36 (2012). It is well-known that the aim of the regulations on liability for fault is not only to reduce any harmful events and to distribute their costs, but also to contain the implementation costs: see G. Calabresi, Costume degli incidenti e responsabilità civile. Analisi economico giuridica (Milano: Giuffrè,
business has led to limited liability for providers.\(^4\) The use of criteria based on subjective elements for attributing behaviour has served to spread digital literacy and make the web a particularly attractive market.

The privilege given to the economic aspect of the issues in question is demonstrated by the supervisory authorities’ inaction regarding flagrant violations of individual freedom, which only emerged in the Schrems case thanks to the obstinacy of a young university student.

Thus, market logic has dominated the protection of the rights and freedom of people. However, the future appears to hold timid regulatory efforts and forms of ‘constitutionalisation’ of the means of protection.\(^4\) They include attempts to carry out reforms aimed at building a system of fairer rules, more attentive to the needs of individuals, (who will no longer be viewed as mere ‘users’), and based on a logical and yet not acceptable categorisation based on status.\(^4\)


\(^4\) It is worth considering, for example, the Declaration of Rights on the Internet of 28 July 2015, approved by the Commission for the rights and duties on the Internet of the Italian Chamber of Deputies.

\(^4\) The consideration of P. Perlingieri is illuminating, Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti (Napoli: Edizioni Scientifiche Italiane, 2006), 663. It is worth recalling that on the issue of status, ‘the doctrine has reserved an alternative attention. The greatest danger lies in making undue generalisations, identifying that a vague and general notion of status in which to insert realities and situations that are very different, forgetting the particular features of each case’. For a reconstruction of the concept in the doctrine, see G. D’Amelio, ‘Capacità e “status” delle persone’, in S. Rodotà ed, Il diritto privato nella società moderna (Bologna: Il Mulino, 2nd ed, 1977), 139; P. Rescigno, ‘Situazione e status nell’esperienza del diritto’ Rivista di diritto civile, I, 209-229 (1975); G. Criscioli, ‘Variazioni e scelte in tema di status’ Rivista di diritto civile, I, 157-209, 185 (1984); A. Corasaniti, ‘Stato delle persone’ Enciclopedia del diritto (Milano: Giuffrè, 1990), XXIII, 948-977; G. Alpa, Status e capacità. La costruzione giuridica delle differenze individuali
Effectively, a process has been set in motion to ensure a harmonious evolution of the internet. The web is only one dimension of the reality in which we all live; it is an aspect of the environment in which the person is formed. If everything can be shared, the virtual space cannot be a no-man’s land, abandoned to spontaneously determined forms of regulation. There is no ‘invisible hand’ influencing the behaviour of the parties.\textsuperscript{43} Rules are the basis of democratic life, and the internet as a realm of social interaction cannot escape from the principles and values of the legal system.\textsuperscript{44}

V. Sustainable Development of the Web: Corporate Social Responsibility in the Information Society

Having realised that the internet is part of the environment in which individuals live, we must commit to ensuring its sustainable development, in its broadest sense.\textsuperscript{45} In this sense, the Schrems case is an exemplar. No matter how attractive the potential of science and technology to improve the quality of human relationships, internet usage cannot be governed solely by corporate and market logic; rather, it requires careful regulation.\textsuperscript{46} This should prevent

\begin{itemize}
\item \textsuperscript{43} Contemporary society has significantly evolved from the one observed by Adam Smith in \textit{An Inquiry into the Nature and Causes of the Wealth of Nations} of 1776, available at http://www.ifarchive.com/pdf/smith__an_inquiry_into_the_nature_and_causes_of_the_wealth_of_nations%5Bi%5D.pdf (last visited 6 December 2016).
\item \textsuperscript{44} In general, see P. Perlingieri, ‘Complessità e unitarietà dell’ordinamento giuridico vigente’ \textit{Rassegna di diritto civile}, 188-214 (2005); and Id, \textit{Il diritto civile nella legalità costituzionale} n 42 above, 159-215.
\item \textsuperscript{46} A regulatory effort that is not simple, considering the distances between the legal systems involved. For example, in the processing of sensitive data, the European perspective is very different from that of North America. If compared with the EU, the US regulatory environment is weaker, with respect to three main issues: restricting access to personal data on intelligence (once acquired by public authorities); law user protection with regard to
private and public behaviour which, although technically legitimate, may be harmful to personal freedoms.

For example, the protection afforded to privacy with regard to the transfer of data to third countries, to date has not been very attentive to the enunciation of general mandatory principles ensuring the protection of the individual. This is a fact that should make legislators reflect, especially at the European level, when dealing with globalised and ever-changing cases.  

For example, it is not possible to nurture particular expectations about the future application of the new European regulation on the processing of personal data. Even if the regulation is in accordance with an extensive legislation on data transfers to third countries (Arts 44-50), it will still need to create new and significant solutions for the events that may arise.

It is also worth mentioning the non-negligible concern that the application of the aforementioned regulations has been postponed to 25 May 2018, a very long implementation period when considering the speed with which technological progress offers new communication tools.

To conclude, in light of the above, it is possible to perceive an underlying common concern, namely ensuring the continuation of business, since the facts described negatively affect its performance. It is therefore worth

---


remembering that information society services are only apparently free.\textsuperscript{49}

Usage is the compensation they receive for the services they provide, monetised by the company through the sale of advertising space.\textsuperscript{50} All of this is certainly permissible, provided that the cost for using these services is not an unreasonable compression of individual liberties.

It may be worth recalling that companies carry out their activities in a social context and answer socially for their actions.\textsuperscript{51} The responsibility system on the internet must therefore be a system of obligations that is not only public, but above all, private. It is not necessary to invent this system from scratch, since it is possible to refer to known concepts, such as corporate social responsibility.\textsuperscript{52}

Thus, service providers must do business by satisfying user requirements while knowing, at the same time, how to manage the expectations of the other stakeholders in the operating environment. This may bring order to the chaos of cyberspace.

\textsuperscript{49} An issue dealt with by C. Perlingieri, n 36 above, 92.

\textsuperscript{50} Once again, as highlighted ibid. For a description of the characteristics of the information market, for all, see the considerations expressed by V. Zeno-Zencovich, ‘A Comparative Reading of the 675/96 on the Processing of Personal Data’, in V. Cuffaro, V. Ricciuto and Id eds, \textit{Trattamento dei dati e tutela della persona} (Milano: Giuffrè, 1998), 159-168.
