The Digital Single Market and the regulation of personal data

Catherine Barreau, professor of corporate law at the School of Law and Political Science, University of Rennes I

For: In Jean-Pierre Dardayrol (ed.) *The European digital union* [special issue of *Réalités Industrielles*, August 2016] for Web http:??? 2016.

Summary: In 2015, the European Commission issued sixteen proposals for a Digital Single Market. According to several pundits, this market contains a hidden treasure, namely personal data, which firms tap for commercial purposes. Data on individuals' private lives have a special legal status in the EU and member states: they are protected like a fundamental human right. For a long time, a mere directive set the legal framework; but in the spring of 2016, the General Data Protection Regulation was adopted. Will it prove capable of creating the hoped-for balance between the protection of fundamental freedoms (especially with regard to consumers' private lives in a digital economy) and the demands from firms for flexibility and simplicity? As a regulation, this text is uniformly applicable throughout the EU's internal market, but it leaves room for member states to maneuver. This has aroused concern lest a "renationalization" of procedures for protecting personal data impede the realization of a Digital Single Market.

According to a communication bearing the title "A Digital Single Market Strategy for Europe", the European Commission (henceforth EC) states: "*A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise on-line activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.*"[1] Meanwhile, the American GAFA (Google, Apple, Facebook and Amazon) still dominate the digital world market; only YBAT (Yandex, a Russian firm, plus Baidu, Alibaba and Tencent, all Chinese, the last known for WeChat) are effectively putting up a stand.

Europe must settle the tension between, on the one hand protecting personal data and, on the other, promoting a digital domestic market based on the freedom to use data for commercial purposes.[2] For its procedures to be effective, the EU must influence its partners, in particular Switzerland and the United States. While Switzerland is preparing to adjust its legislation to the EU's,[3] the transfer of personal data is a sensitive topic in the United States. After the European Court of Justice overturned the Safe Harbor Privacy Principles in 2015, an agreement was reached on a EU-US Privacy Shield.

[1] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe", §1, COM(2015) 192 final. Available via: http://eur-lex.europa.eu/legal-content/EN/

[2] Article translated from French by Noal Mellott (Omaha Beach, France). References and points of information have been updated for this translation.

[3] http://dievolkswirtschaft.ch/fr/2015/10/2015-11-montereale/

After public hearings during the second semester of 2015 were held to gauge stakeholders' opinions, the EC adopted several texts during the first semester of 2016; and other texts are to follow by the end of the year. There has been a delay in adopting certain measures, and several professionals in e-businesses have doubts about the eventual effectiveness of proposed measures. In legal circles, this process has bred scepticism.

As the first part of this article shows, the diffusion of regulations on personal data as part of the Digital Single Market (henceforth DSM) strategy is operational. As shown in the second part however, there are problems with fitting the regulation about protecting personal data into the rationale for an "internal market".

The diffusion of rules on personal data as part of the DSM strategy

The Digital Single Market strategy has three pillars, each of which has three actions that will lead to sixteen measures. At least one action of each pillar has to do with personal data.

The first pillar: Improve the access of consumers and firms to digital services and goods in all of Europe

This first pillar implies legislation on transborder markets, a reform of copyright law, the identification of potential problems of competition and the harmonization of value-added tax (VAT) systems (to be proposed by the end of 2016).[4] Two proposals for directives were formulated in 2015: the one about on-line sales contracts[5] and the other about contracts for supplying digital contents.[6] Proposals on e-commerce were presented on 25 May 2016,[7] including one on geographical blockages ("geoblocking") to the growth of markets.[8]

The regulation being proposed[9] will ensure that consumers who are trying to purchase goods or services in another EU country (whether on line or by actually going to a store) should not encounter discrimination in prices, sales conditions or methods of payment unless there is objective justification (owing, for instance, to the VAT or legal measures in the public interest). National

[4] A survey by the *Journal du Net* provides interesting figures for understanding the economic stakes: Flore Fauconnier, "La fragmentation législative et logistique entrave l'e-commerce européen", 1 June 2019. Available at:
http://www.journaldunet.com/ebusiness/commerce/1179389-la-fragmentation-legislative-et-logistique-entrave-l-e-commerce-europeen/

[5] European Commission, "Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the on-line and other distance sales of goods" of 9 December 2015. Available at:
https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-635-EN-F1-1.PDF
See too: Grégoire Loiseau in *Communication Commerce Électronique*, 2016, comment n°23. Available via:
http://unedesrevues.lexisnexis.fr/unerevues/pdf/une/cce1607.pdf

[6] European Commission, "Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content" of 9 December 2015. Available at:
https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-634-EN-F1-1.PDF

[7] European Commission, "Commission proposes new e-commerce rules to help consumers and companies reap full benefit of Single Market", press release of 25 May 2016. Available at:
http://europa.eu/rapid/press-release_IP-16-1887_en.htm

[8] European Commission, "First brief results of the public consultation on geoblocking and other geographically based restrictions when shopping and accessing information in the EU", 27 January 2016. Available at:
https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-geo-blocking-and-other-geographically-based
Geoblocking was illustrated by the Disneyland affair: Jim Brunsden & Duncan Robinson, "Disneyland Paris ditches pricing policy: Theme park alters policy after criticism non-French visitors faced higher fees", *Financial Times*, 15 April 2016.

[9] European Commission, "Proposal for a regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/(22)/EC", 25 May 2016. Available at:
http://ec.europa.eu/DocsRoom/documents/16742/attachments/2/translations/en/renditions/pdf

authorities will verify whether websites practice geoblocking. To avoid disproportionate charges for firms, the proposal does not provide for delivery everywhere in the Union. Some clauses open exemptions for small business below certain (national) VAT thresholds. Nor are services concerned in transportation, retail financing, the audiovisual[10] and music industries, and e-books. However the regulation will be reviewed at the end of a two-year period; and the question of extending it to cover these branches of the economy may then be brought up again.

The EC has published a communication on an agenda for the "collaborative economy".[11] Platforms[12] must propose services under fair conditions of competition. Member states are asked, under the Commission's supervision, to reexamine and, if need be, modify their legislation by taking into account five orientations: conditions of market access; liability in case of legal problems; protection of users under EU consumer legislation; the "existence of a work relationship"; and the fiscal regulations to be applied.

The second pillar: An environment that, favorable to developing innovative services and networks, supports firms while reinforcing the protection of personal data

By the end of 2016, proposals will have been made for: reforming EU regulations about telecommunications; reviewing the Audiovisual Media Services Directive;[13] analyzing the role of on-line platforms in the market (transparency of search findings); and establishing a partnership with industry on cybersecurity[14] in technology and the security of on-line networks. The erection of this pillar is well under way. However work on the most important measure for regulating personal data has barely started, namely the modification of the directive on privacy and electronic communications.[15] The new text containing this modification will have to be articulated with reforms on the protection of personal data.

The third pillar: Maximize the digital economy's potential growth

This third pillar has to do with issues ranging from the protection of personal data to the free circulation of data and the formation of a European cloud. The Commission presented a first set of measures on 19 April 2016[16] that support and link together national programs for making the shift to digital technology in industry and related services in all sectors. It foresees stimulating

[10] In France, television finances the cinema.

[11] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European agenda for the collaborative economy", 2 June 2016. Available at:
http://ec.europa.eu/DocsRoom/documents/16881/attachments/2/translations/en/renditions/pdf

[12] Hosting-providers in the sense of the e-business directive 2001/31/CE.

[13] The Audiovisual Media Services Directive: "Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services". Available via:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478947430193&uri=CELEX:32010L0013
On 25 May 2016, the Commission made a proposal for updating the Audiovisual Media Services Directive. See:
https://ec.europa.eu/digital-single-market/en/news/proposal-updated-audiovisual-media-services-directive

[14] The Council validated the compromise on cybersecurity: Council of the EU, "EU-wide cybersecurity rules adopted by the Council", press release of 17 May 2016. Available at:
http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/

[15] The directive on privacy and electronic communications: "Directive 2002/58EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector". Available via:
http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
A public survey was on line between 11 April and 5 July 2016.
ec.europa.eu/eusurvey/runner/1710fec6-2226-4116-8bc0-a29829d7e1bf?draftid=7eaa51c7-dac9-4c36-8406-7a465a729f6e&surveylanguage=FR

[16] European Commission, "Commission sets out path to digitize European industry", press release of 19 April 2016. Available at:
europa.eu/rapid/press-release_IP-16-1407_fr.htm

investments through strategic partnerships and networks. This has led to modifying the 1995 directive on the free circulation of personal data and the protection of individuals in the case of the processing of personal data.[17] But does this cornerstone of legislative reforms take account of the DSM strategy?

The General Data Protection Regulation: Minimal attention to the DMS strategy

The Maastricht Treaty on European Union (TEU) declared the protection of personal data to be a new fundamental right in line with Article 8 of the Charter of Fundamental Rights of the European Union. Confirming this, Article 16 of the Treaty on the Functioning of the European Union (TFEU) empowers the European Parliament and Council to adopt regulations about protecting persons with regard to the processing and circulation of their personal data. The set of measures on data protection includes a directive about transferring data to the police or judicial authorities.

The General Data Protection Regulation (henceforth GDPR) was published in the *Official Journal of the European Union* on 4 May 2016.[18] Applicable twenty days after publication, the GDPR will replace Directive 95/46/CE in two years. Recital 171 of its preamble states that the passage from one set of rules to another will not be sudden. The data-processing procedures in use at the time of enforcement of the GDPR will have two years to be made compliant.

Despite its ambition, the GDPR as adopted is a compromise. As a result of intense lobbying with a clearly perceptible influence, the final version differs significantly from draft versions. It leaves an amazing latitude to member states. This represents a risk for the success of the DMS strategy.

Though intended to protect data, the GDPR seems, at first sight, hardly favorable to the commercialization of personal data. However certain clauses mention an "internal market".

Reading the GDPR lets us see the continuity between the old and new regulations. Basic definitions (Article 4) have been carried over; the rights of individuals have been clarified and augmented; and the obligations of data-processors have been updated.

The processing of personal data is not lawful unless the person concerned has given clear and affirmative consent after receiving precise information in simple and clear terms about the purposes of the processing. The person may refuse profiling and invoke a right to be forgotten ("right to erasure"), which has more solid grounds than the "right to delinking" validated by the Court of Justice of the European Union (CJEU) in its Google ruling. The GDPR enshrines the right to data portability (in particular, when changing providers). Exercising these rights is for free. Strict conditions have been set for transferring data collected in third countries.

[17] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Available via:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=fr

[18] General Data Protection Regulation: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC". Available via:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679
L119 in the *Journal*. Available via:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

In parallel, when designing data-processing techniques, firms must protect the data though "*privacy by design*", which sets the principle of security as the default. They are held to appoint "*data protection officers*", adopt codes of conduct, follow certification procedures and notify security holes to supervisory authorities and the persons concerned. Depending on the violation, if confirmed, an administrative fine may be set of up to ten or twenty million euros or, in the case of a firm, of from 2% to 4% of its total annual sales worldwide during the preceding period (the highest amount being retained).

These rules attest to the determination not only of the Commission but also of nonprofit organizations, as expressed during public hearings, to restore to individuals control over their own data. Doubts have been voiced about how effective these rules will be. Will the rules about consent be applied, given that, nowadays, the consent requested seems illusory?[19] Is privacy by design an effective technique,[20] given that "pseudonymization" does not provide real protection?[21] Nor does the GDPR settle the issues related to big data.[22]

Firms have not objected very much to the GDPR. According to some studies, they are not even aware of it. Nor did its publication arouse much attention, at least not in the French press.

The GDPR provides an auspicious framework for the DMS strategy. For instance, the clauses on its extraterritorial application endow firms with new means for resisting the GAFA.

The GDPR applies to parties responsible for processing data that are established in the European Union or, too, outside the Union if this processing involves data about EU residents (Article 3). This significantly new provision will reinforce the EU's authority in negotiations with firms and public authorities outside the Union. Non-EU countries might see it as a violation of their sovereignty. Bear in mind, however, that the supervisory and regulatory powers of the EU and its member states cannot be exercised outside EU borders. Even though the situation resulting from the Google jurisprudence has now been clarified, European firms still cannot hope to stand on an equal footing with the American giants.

Although Article 27 stipulates that the "*controllers*" or "*processors*" of personal data established outside the EU must "*designate in writing a representative in the Union*", this obligation applies neither to occasional data-processing nor to public authorities. Instead of making EU regulations more effective, this article, given the fuzziness of its first exception, might be a cause of legal insecurity, since it lets to foreign firms the diligence of determining whether or not they meet up to the GDPR's obligations. The political dimension explains the general formulation used for the second exception. Any other solution would have occasioned major diplomatic problems. The only way to ensure the protection of personal data is to adopt in a far-off, uncertain future an international convention on the topic.

Firms will benefit from a "*one-stop-shop mechanism*". They will have dealings with a single supervisory authority in charge of applying the GDPR. This simplification is a blessing for the small and medium-sized firms that do not fall under the general exemption foreseen under Article 30-5 for firms or organizations with fewer than 250 employees. EU institutions, member states and their supervisory authorities are, however, advised to take into consideration the "*specific needs of micro, small and medium-sized enterprises*". This is an invitation for member states to take advantage of the room to maneuver allowed under the GDPR.

---

[19] M. Boizard, "Le consentement à l'exploitation des données à caractère personnel: une douce illusion?", *Communication Commerce Électronique*, 3(6), March 2016.

[20] A. Rallet, "De la 'privacy by design' à la 'privacy by using'", *Regards croisés Droit/économie*, *Réseaux*, 89, pp.15-46, 2015.

[21] wiki.laquadrature.net/Synth%C3%A8se_du_r%C3%A8glement_sur_la_protection_des_donn%C3%A9es/en

[22] S. Vulliet-Tavernier, "*Big data* et protection des données personnelles: quels enjeux? (éléments de réflexion)", *Statistique et société*, 2(4), p.27ff. December 2014; and V. Mayer-Schönberger, "La Révolution *big data*", *Politique étrangère*, 4, pp.69-81, 2014.

A regulation, as the law of the EU, is applicable to all member states; yet the GDPR lets room for member states to adopt their own arrangements.

The legal instrument preferred for addressing the issue of personal data is a regulation, instead of a directive. In effect, a regulation provides a coherent level of protection to natural persons everywhere in the EU. Furthermore, it shields the free flow of data on the "*internal market*" from infringement by national rules and regulations.

The principles, once laid down in Recital 9 of the preamble, are just as soon qualified under Recital 10, which lets members states the possibility of being dispensed from the GDPR in case of several sorts of data-processing on a national or "*sector-specific*" basis. This margin of maneuver is recognized in cases of processing personal data "*for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" and "*for special categories of personal data ('sensitive data')*".

These very specific formulations open a wide gap in the unification of legal rules at the EU level. But the gap also yawns in common points that, given the stated objectives, should have been part of a uniformization. There is a major risk lest member states adopt their own rules such that national laws diverge as much as, or even more than, they now do. This will create an insecure legal environment for firms.[23] Companies will have to take into account each member state's rules to make sure that their processing of personal data is lawful — contrary to the one-stop-shop principle promised by the GDPR.

The risk of national laws diverging might be limited by the requirement of prior consultation under Article 36-4, whereby member states must consult the "*supervisory authority during the preparation of a proposal* [about processing personal data] *for a legislative measure to be adopted by a national parliament*".

Supervisory authorities are to work closely together and will, therefore, be able to attract the attention of member states to potential legislative differences and their eventual consequences. They are to cooperate and assist each other and even act together (articles 60ff). There is, too, a "*consistency mechanism*" (articles 63ff) under the European Data Protection Board, whose makeup and tasks are defined by articles 68ff.

The GDPR contains a long list of recitals in its preamble, which, by definition, is not compulsory. Certain key points figure in the preamble, not among the articles.

Some of these recitals contain measures that could have, if an agreement had been found, been placed among the regulation's enacting terms. Is there the risk of a creeping "renationalization" — to the detriment of the Digital Single Market? Recital 53 calls for special attention since it is necessary for the interpretation of Article 17 on the right to erasure. In the interest of natural persons and of firms, it should have listed all the points required for its application. We will have to wait until the CJEU clears up the uncertainty by ruling on this point.

[23] "New EU data protection rules increase administrative burden", press release of BusinessEurope on 14 April 2016. Available at: www.businesseurope.eu/sites/buseur/files/media/press_releases/2016-04-14_pess_release_on_data_protection_regulation.pdf