ON THE WATERFRONT: PERSONAL AND NON-PERSONAL DATA AT BOTH EU REGULATIONS

Manuel David Masseno

Abstract: European Union Law on data protection does not apply to non-personal data. However, the legal limits between personal and non-personal data are unstable, relying on the development of anonymization and desanonymization technologies, with increasing risks to be handled by controllers and processors. This paper intends to identify the mentioned risks and the possible remedies, according to the General Data Protection Regulation.

Keywords: European Union. Non-personal data. Personal data. Regulation. Risk.

Resumo: O Direito da União Europeia sobre proteção de dados não se aplica aos dados não pessoais. Porém, os limites legais entre dados pessoais e dados não pessoais são instáveis, assentando no desenvolvimento de tecnologias de anonimização e de desanomnizização, com riscos crescentes para controladores e operadores. Este artigo pretende identificar os riscos mencionados e as respostas possíveis, de acordo com o Regulamento Geral de Proteção de Dados.


1 LAND AND SEA

For starters, this short paper was built having in mind an ancient maritime cartographic metaphor that has a remarkable heuristic potential, given the current state of EU Sources regarding the regulation of data, both personal and non-personal: hic sunt dracones, the sea monsters that were supposed to populate uncharted waters.

1 Texto da Comunicação apresentada na Nordic Conference on Legal Informatics 2019, realizada na Universidade da Lapónia, em Rovaniemi (Finlândia), entre os dias 12 e 14 de novembro de 2019. Apenas foram acrescentadas as notas e as Referências bibliográficas, as quais se restringem à Europa e às Línguas Inglesa e Portuguesa.

Besides, being this a “Nordic Conference”, taking place at Rovaniemi, the Carta Marina, of Olaus Magnus / Olof Månsson, dating from 1539, other than the Atlantic and Arctic Oceans, shows one of the first known and accurate representations of Scandinavia and the Baltic, including Lapland.

As a matter of fact, if we take a closer look to the EU Sources, we will notice that there’s in place a detailed and consistent set of rules regarding Personal Data, Terra Firma, based on Regulation 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 (General Data Protection Regulation) – the GDPR.

This Continent is bordered by a Sea of loose and unsettled rules, notwithstanding Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November

3 In full, Carta marina et Descriptio septemtrionalium terrarum ac mirabilium rerum in eis contentarum, diligentissime elaborata Anno Domini 1539 Veneciis liberalitate Reverendissimi Domini Ieronimi Quirini, written during his exile in Italy and available here: http://www.npm.ac.uk/rsdas/projects/carta_marina/carta_marina_small.jpg.

4 Another Continent, or rather a few rocky islands, as to do with the EU legal answers towards Cybercrime, namely Directive 2011/93/EU, of the European Parliament and the Council of 13 December 2011, on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013, on attacks against information systems, both aiming to consolidate the Council of Europe Convention on Cybercrime, ETS No. 185, signed at Budapest the 23rd November 2001, and its complementing framework, as the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, signed at Strasbourg the 1st March 2003, and the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, signed at Lanzarote, the 25th October 2007.

2018, on a framework for the free flow of non-personal data in the European Union – the FFD Regulation.

Our subject is akin to a Waterfront, where Terra Firma and the Sea met dynamically, under the effect of technological tides.

2 EVEN ON WETLANDS

As well known, the GDPR “applies to the processing of personal data” (Article 2.1), not just of an “identified person” but also relating to an “identifiable natural person”, “[that is] one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Article 4.1), including quasi-identifiers and metadata (Article 4.1), as “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags […]” (Recital 30).

Concluding that “[…] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes” (Recital 26 in fine).

In addition and regarding this subject, we should keep in mind the Breyer Case Law of the Court of Justice of the European Union⁶.

Later and on the other hand, the **FFD Regulation** clarified that it “applies to the processing of electronic data other than personal” (Article 2.1). Intending to address the legal issues resulting from “The expanding Internet of Things, artificial intelligence and machine learning, [that] represent major sources of non-personal data, for example as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines.” (Recital 9).

However, the **GDPR** keeps a strong *vis atractiva*. So, “In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679” (Article 2.2).

### 3 BUT, EVENTUALLY, THE TIDE RETREATS

Concerning des-anonymization, **Directive 95/46/EC**, relied on a *legal fiction*, stating that “[…] whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable […] and retained in a form in which identification of the data subject is no longer possible” (Recital 26), implying the irreversibility of anonymization.

Though, that’s no longer the case for the **GDPR**. Following what we’ve seen, “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols […]. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.” (Recital 30)

On the other hand, the **FFD Regulation** is limpid, “If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly” (Recital 9 in fine).

Meanwhile, EU Institutions became quite aware of these facts, at least by the Opinions of the **Article 29 Working Party**, as [Opinion 7/2003](#) on the re-use of public sector information and the
protection of personal data, of 12 December 2003, Opinion 06/2013 on open data and public sector information (‘PSI’) reuse, of 5 June 2013\(^7\), and, above all, Opinion 05/2014 on “Anonymisation Techniques”, of 10 April 2014.

The same for some National Supervisory Authorities, such as the UK Information Commissioner’s Office, with the “Anonymisation: managing data protection risk code of practice”, of November 2012, or the Agencia Española de Protección de Datos, with the “Orientaciones y garantías en los procedimientos de anonimización de datos personales”, of October 2016.

For its part, the Commission came forward and issued a “Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union” (COM/2019/250 final, of 29 May 2019), with specific and clear references to the data protection risks coming from des-anonymization technologies (2.1).

And the Report (A/HRC/31/64), of 24 November 2016, delivered by the Special Rapporteur on the rights to privacy, Prof. Joseph Cannataci to the Office of the UN High Commissioner for Human Rights, also has to be mentioned.

Furthermore, along the last decade, Academia has shown the limits of anonymization. Already in 2010, Paul Ohm exposed the shortcoming of the available techniques, and, last July, from a mathematical approach, a group of Belgian researchers from the University of Leuven and the Imperial College, London, Luc Rocher, J.M. Hendrickx & Y.-A. de Montjoye, demonstrated how easily (re)identification can be achieved\(^8\).

### 4 PRECAUTIONS TO TAKE BEFORE BOARDING

In order to identify the coastal rocks to be covered during the high tides, before any processing of non-personal data, the Captain (Controller) and the Pilot (Data protection officer)
should perform risk evaluations, in order to “ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.” (Recital 26)\(^9\).

Being implied by the *Principle of Accountability* (Article 5.2 of the *GDPR*)\(^{10}\), these evaluations should follow the stated criteria concerning “Data protection by design and by default” (Article 25)\(^{11}\) and, if necessary, a “Data protection impact assessment” (Article 35)\(^{12}\) has to be performed.

Additionally, “an approved certification mechanism pursuant to Article 42” (as stated at Article 25.3 considering “data protection by design and by default” and at Article 32.2 in relation to the “security of processing”) could be utterly relevant in order to avoid major *rocks*\(^{13}\).

A completing tool could be, when available, an “European cybersecurity certification scheme”, particularly one providing a ‘substantial’ or a ‘high’ assurance level (as at Art. 52 of *Regulation (EU) 2019/881* the European Parliament and of the Council of 17 April 2019, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act)\(^{14}\).

## 5 PREVENTING MARITIME INCIDENTS

\(^9\) For the role performed by these evaluations, Niels van DIJK, Raphaël GELLERT and Kjetil ROMMETVEIT (2016), as well as Raphaël GELLERT (2018).


\(^{12}\) For a synthesis, Niels van DIJK, Raphaël GELLERT and Kjetil ROMMETVEIT (2016), notwithstanding the *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, from the Article 29 Working Party, of 4 April 2017, revised on 4 October 2017.

\(^{13}\) Apart from the very recent *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3.0)*, of 3 June 2019, adopted by the European Data Protection Board, for a general approach to this subject, Giovanni Maria RICCIO and Federica PEZZA (2018), as well as Eric LACHAUD (2018).

\(^{14}\) On the European Union Cybersecurity framework, Helena CARRAPIÇO and André BARRINHA (2017) and (2018), more specifically but from a somewhat outdated perspective, Roksana MOORE (2013), while Christopher CUNER *et al.* (2017) put the focus on its connections with data protection.
In order to avoid shoals, “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data” (Article 35.1), following the state of the art on the (re)personalization of data.

Though, the most effective procedure would be drainage of the relevant part of the shore, that is, to apply the GDPR to ALL processing of data, personal and non-personal, at least when technologies such as “Internet of Things, artificial intelligence and machine learning” (Recital 9 of FFD Regulation) are being used. Starting with encryption (Article 32.1 a)\(^\text{15}\), at least, in order to limit the consequences of a “personal data breach” (Article 34.3 a) and Article 4 12)\(^\text{16}\).

REFERENCES


\(^{15}\) About these, Gerald SPINDLER and Philipp SCHMECHEL (2016), in general, as well as Samson Y. ESAYAS (2015), for the precise context.

\(^{16}\) About the scope of the rules regarding these security incidents, Stephanie von MALTZAN (2019).


HANSEN, Marit; LIMNIOTIS, Konstantinos. Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default. ENISA – European Union Agency for Cybersecurity, jan. 2018. Available in:


