ISSN: 1982-5552

Revista Jurídica da FADISMA

ON THE WATERFRONT: PERSONAL AND NON-PERSONAL DATA AT BOTH EU REGULATIONS[1]

Manuel David Masseno[2]

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 desanonimização, 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.
Palavras-chaves: Dados não pessoais. Dados pessoais. Regulação. Risco, União Europeia.

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.

[2] Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança de Segurança Informática. Pertence à EDEN Rede de Especialistas em Proteção de Dados da Europol Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, em Portugal; assim como ao Grupo de Estudos de Direito Digital e *Compliance* da FIESP - Federação das Indústrias do Estado de São Paulo, à Comissão Estadual de Direito Digital da Ordem dos Advogados do Brasil, Seção de Santa Catarina, é ainda Coordenador de Direito Digital Comparado na Comissão de Direito digital da Subseção de Campinas da OAB e Membro Honorário do Instituto IDEIA – Instituto Direito e Inteligência Artificial.

ISSN: 1982-5552

Revista Jurídica da FADISMA

Besides, being this a "Nordic Conference", taking place at Rovaniemi, the *Carta Marina*[3], 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*[4].

This *Continent* is bordered by a *Sea* of loose and unsettled rules[5], 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.

[5] Also having in mind the EU *Archipelago* of Intellectual Property Acts, with a *reef*, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004, on the enforcement of intellectual property rights; *sandbanks*, as Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, on the harmonisation of certain aspects of copyright and related rights in the information society, and Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019, on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC; and some *islands* apart like Council Directive 91/250/EEC of 14 May 1991, on the legal protection of computer programs, Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996, on the legal protection of databases, Directive 98/71/EC, of the European Parliament and of the Council of 13 October 1998, on the legal protection of designs, also Council Regulation (EC) No 6/2002 of 12 December 2001, on Community designs, Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998, on the legal protection of biotechnological inventions, Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012, implementing enhanced cooperation in the area of the creation of unitary patent protection, both complementing the *Convention on the Grant of European Patents*, of 5 October 1973, Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017, on the European Union trade mark, Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015, to approximate the laws of the Member States relating to trade marks, Regulation (EU) No 1151/2012 of the European Parliament and of the Council of 21 November 2012 on quality schemes for agricultural products and foodstuffs and Regulation (EU) 2018/848 of the European Parliament and of the Council of 30 May 2018, on organic production and labelling of organic products;

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 Union[6].

and a *marsh*, Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[6] Namely, after Case C-582/14, Patrick Breyer, of 19 October 2016, reiterated at Case C-434/16, Peter Nowak, of 20 December 2017, preceded by *Article 29 Working Party* Opinion 4/2007, on the concept of personal data, of 20 June 2007. About these issues, Paul SCHWARTZ and Daniel SOLOVE (2011), Frederik Zuiderveen BORGESIUS (2017), Nadezhda PURTOVA (2018) and Lorenzo dalla CORTE (2019).

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)

[7] On the tension concerning open data, the reuse of public sector data and data protection, Katleen JANSSEN and Sara HUGELIER (2013).

[8] On the issue, Paul SCHWARTZ and Daniel SOLOVE (2011), again Daniel SOLOVE (2014), Samson Y. ESAYAS (2015), Sophie STALLA-BOURDILLON and Alison KNIGHT (2017), and also, from technological perspective, Arvind NARAYANAN and Vitaly SHMATIKOV (2008); and a special attention has to be provided to Big Data Analytics, as shown by Benjamin HABEGGER *et al*. (2014), Jens-Erik MAI (2016), Alessandro MANTELERO, (2016), Nils GRUSCHKA *et al*. (2018), and also by my paper with Cristiana Teixeira SANTOS (2019).

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).

[10] About its scope, besides *Article 29 Working Party* Opinion 3/2010 on the principle of accountability, of 13 July 2010, Lachlan URQUHART, Tom LODGE and Andy CRABTREE (2019).

[11] Besides the reports commissioned by ENISA to George DANESIS *et al*. (2014), to Giuseppe D'ACQUISTO *et al*. (2015) and to Marit HANSEN and Konstantinos LIMNIOTIS (2018), the papers by Lee A. BYGRAVE (2017), Irene KAMARA (2017) and Filippo A. RASO (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)[15], at least, in order to limit the consequences of a "personal data breach" (Article 34.3 a) and Article 4 12)[16].

REFERENCES

BORGESIUS, Frederik Zuiderveen. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition, **European Data Protection Law Review**, v. 3, n. 1, p. 130-137, 2017. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933781

BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, **Oslo Law Review,** v. 4, n. 2, p. 105-120, 2017. Available in: https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_

CARRAPIÇO, Helena; BARRINHA, André. The EU as a Coherent (Cyber)Security Actor? **Journal of Common Market Studies**, v. 55, n. 6, p. 1254–1272, 2017. Available in: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12575

CARRAPIÇO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. **European Politics and Society**, v. 19, n. 3, p. 299-303, 2018. Available in: https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712

[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).

CORTE, Lorenzo Dalla. Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law. **European Journal of Law and Technology**, v. 10, n. 1, 2019. Available in: http://ejlt.org/index.php/ejlt/article/view/672

CUNER, Christopher *et al*. The rise of cybersecurity and its impact on data protection **International Data Privacy Law**, v. 7, n. 2, p. 73-75, 2017. Available in: https://www.repository.law.indiana.edu/facpub/2633/

DANESIS, George *et al*. **Privacy and Data Protection by Design – from policy to engineering.** ENISA - European Union Agency for Cybersecurity. dec. 2014. Available in: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

D'ACQUISTO, Giuseppe *et al*. **Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics.** ENISA - European Union Agency for Cybersecurity. dec. 2015. Available in: https://www.enisa.europa.eu/publications/big-data-protection

DIJK, Niels van; GELLERT, Raphaël; ROMMETVEIT, Kjetil. A risk to a right? Beyond data protection risk assessments. **Computer Law & Security Review**, v. 32, n. 2, p. 286-306, feb. 2016. Available in: https://www.researchgate.net/publication/294577405_A_risk_to_a_right_Beyond_data_protection_risk_assessments

ESAYAS, Samson Yoseph. The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. **European Journal of Law and Technology**, v. 6, n. 2, 2015. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746831

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law and Security Review**, v. 34, n. 2, p. 279-288, 2018. Available in: https://www.sciencedirect.com/science/article/abs/pii/S0267364917302698

GRUSCHKA, Nils *et al*. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. **Proceedings of the 2018 IEEE International Conference on Big Data**, Seattle, nov. 2018. Available in: https://arxiv.org/pdf/1811.08531.pdf

HABEGGER, Benjamin *et al*. Personalization vs. Privacy in Big Data Analysis. **International Journal of Big Data**, v. 1, p. 25-35, jan. 2014. Available in: https://www.researchgate.net/publication/295121842_Personalization_vs_Privacy_in_Big_Data_Analysis

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:

https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

JANSSEN, Katleen; HUGELIER, Sara. Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive. **European Journal of Law and Technology**, v. 4, n. 3, 2013. Available in: https://www.semanticscholar.org/paper/Open-data-as-the-standard-for-Europe-A-critical-of-Janssen-Hugelier/345b0f11f2195fd21e72eb678d1357343044b387

KAMARA, Irene. Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. **European Journal of Law and Technology**, v. 8, n. 1, mar. 2017. Available in: https://research.tilburguniversity.edu/en/publications/co-regulation-in-eu-personal-data-protection-the-case-of-technica

LACHAUD, Eric. The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument **Computer Law and Security Review**, v. 43, n. 2, pp. 244-256, mar. 2018. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940805

MAI, Jens-Erik. Big data privacy: The datafication of personal information. **The Information Society,** v. n. 32, n. 3, pp. 192-199, apr. 2016. Available in: http://jenserikmai.info/Papers/2016_BigDataPrivacy.pdf

MALTZAN, Stephanie Von. No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protection Compliant Incident Response System. **European Journal of Law and Technology,** v. 10, n. 1, 2019. Available in: http://ejlt.org/index.php/ejlt/article/view/665/893

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. **Computer Law & Security Review**, v. 22, n. 2, p. 238-255, 2016. Available in: https://www.academia.edu/25657426/Personal_data_for_decisional_purposes_in_the_age_of_analytics_From_an_individual_to_a_collective_dimension_of_data_protection

MASSENO, Manuel David; SANTOS, Cristiana Teixeira. Personalization and profiling of tourists in smart tourism destinations - a data protection perspective. **International Journal of Information Systems and Tourism**, v. 4, n. 2, p. 7-23, 2019. Available in: http://www.uajournals.com/ijist-tourism/journal/4/2/1.pdf

MOORE, Roksana. The Case for Regulating Quality within Computer Security Applications **European Journal of Law and Technology,** Vol. 4-3, 2013. Available in: http://ejlt.org/article/view/272/412

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets **IEEE Symposium on Security and Privacy,** Oakland, 2008. Available in: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. ***UCLA Law Review,*** v. 57, p. 1701-1777, 2010. Available in: https://www.uclalawreview.org/pdf/57-6-3.pdf

PURTOVA, Nadezhda. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. **Law, Innovation and Technology,** v. 10, n. 1, p. 40-81, 2018. Available in: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

RASO, Filippo A. Innovating in Uncertainty: Effective Compliance and the GDPR. **Harvard Journal of Law & Technology Digest,** 2018. Available in: https://jolt.law.harvard.edu/assets/digestImages/PDFs/Raso_2018-08.pdf

RICCIO, Giovanni Maria; PEZZA, Federica. Certification Mechanism as a Tool for the Unification of the Data Protection European Law. **MediaLaws – Rivista di diritto dei media,** n. 1, pp. 249-260, 2018. Available in: http://www.medialaws.eu/wp-content/uploads/2019/05/18.-Riccio-Pezza.pdf

ROCHER, Luc; HENDRICKX, Julien M.; MONTJOYE, Yves-Alexandre de. Estimating the success of re-identifications in incomplete datasets using generative models **Nature Communications,** v. 10, dec. 2019. Available in: https://www.researchgate.net/publication/334634583_Estimating_the_success_of_re-identifications_in_incomplete_datasets_using_generative_models

SCHWARTZ, Paul; SOLOVE, Daniel. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. **New York University Law Review**, v. 86, p. 1814-1894, 2011. Available in: https://papers.ssrn.com/sol3/PIP_Journal.cfm?pip_jrnl=215051

SCHWARTZ, Paul; SOLOVE, Daniel. Reconciling Personal Information in the United States and European Union. **California Law Review,** v. 102, p. 877-916, 2014. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442

SPINDLER, Gerald; SCHMECHEL, Philipp. Personal Data and Encryption in the European General Data Protection Regulation. **JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law**, v. 7, 2016. Available in: https://www.jipitec.eu/issues/jipitec-7-2-2016/4440

STALLA-BOURDILLON, Sophie; KNIGHT, Alison. Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. **Wisconsin International Law Journal,** v. 34, n. 2, p. 285-322, mar. 2017. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy. Demonstrably doing accountability in the Internet of Things. **International Journal of Law and Information Technology**, v. 27, n. 1, p. 1-27, 2019. Available in: https://academic.oup.com/ijlit/article/27/1/1/5259368