Revista da Faculdade de DIREITO da Universidade Federal de Uberlândia

The Right of Data Portability in EU's GDPR and Brazil's LGPD

O Direito à Portabilidade de Dados no RGPD e na LGPD

Daniela Copetti Cravo[1]

Abstract: At the same time that data portability is one of the greatest innovations brought by contemporary data protection legislation, it also represents one of the market's greatest challenges. Concerns about data transmission or interoperability safety are inevitable, as well as about compliance costs. Thus, innumerable doubts arise regarding the aspects of data portability implementation and its peculiarities. In this sense, the paper aims to analyze the most critical points of data portability in the Brazilian context based on comparisons of other legal systems experience, especially that of the European Union.
Keywords: Data portability.Implementation, Data protection legislation.

Resumo: Ao mesmo tempo em que a portabilidade é uma das maiores inovações trazidas nas contemporâneas legislações de proteção de dados, essa também representa um dos maiores desafios ao mercado. Preocupações quanto à segurança na transmissão dos dados ou quanto à interoperabilidade são inevitáveis, bem como com relação ao custo do compliance. Assim, inúmeras dúvidas surgem quanto à forma de implementação da portabilidade de dados e aos seus contornos. Nesse sentido, a proposta desse artigo é justamente analisar os pontos mais críticos da portabilidade de dados no contexto brasileiro, a partir da experiência comparada de outros ordenamentos e sistemas.
Palavras-chave: Portabilidade de Dados.Implementação.Legislação de proteção de dados pessoais**.**

1. Introduction

The development of personal data protection in Brazil is marked by legislative delay on the enactment of a general, contemporary and adequate law to a digital reality and by the inertia on creating a regulatory authority on the matter of data protection. This reality could be considered long

[1] Procuradora do Município de Porto Alegre. Diretora Acadêmica da ESDM. Doutora e Mestre em Direito pela UFRGS. Pós-Doutorado no Departamento de Direito Público e Filosofia do Direito da Faculdade de Direito da UFRGS (2019 - 2020). Professora da Faculdade de Direito da São Judas Tadeu. Více-Líder do Grupo de Pesquisa Comércio Internacional, mercados, investimentos internacionais e circulação de riquezas. Visitante de Investigação na Facultad de Derecho da Universidad de Chile.

DOI: https://doi.org/10.14393/RFADIR-50.1.2022.62778.89-121

overdue not only when comparing Brazil to European countries, but also to other Latin American countries.

Such a legal anomie, however, has begun to change in the last couple of years in light of considerable advances in data protection. In 2018, the Brazilian General Data Protection Act - LGPD (Lei nº 13.709/2018) was enacted. Subsequently, in 2019, it was proposed a constitutional amendment (PEC - Constitutional Amendment Proposal -17/2019) that seeks to place data protection as a fundamental right and to establish legislative competence on the matter only to the Federal Union. Now, in 2020, there was a lead ruling by the Brazilian Federal Supreme Court - (Medida Cautelar da ADI 6387), where personal data protection was recognized as a fundamental right.

Therefore, it is possible to say that persontastes, a protection is already a reality in Brazil, even more with the LGPD coming into force on the 18th of September 2020. This law will inaugurate a series of novelties in the Brazilian legal system, as such as: the uniformity and the transversality of the legal treatment on the subject-matter, in a clear way to guarantee legal certainty and to fight off legal fragmentation and the creation of a legal ground that legitimate personal data processing.

Besides, the LGPD also gives data subjects a myriad of rights. Among these rights, it is highlighted the right to personal data portability, which was inspired by the novelty (BOZDAG, s.d.) provided through the article 20 of the General Data Protection Regulation (GDPR)2.

Data portability, understood as the possibility of the data subject to transfer its data between different data controllers or to obtain a copy for

[2] The right to data portability was provided through the Proposal presented by the European Parliament and by the Council, dated 25th of January 2012, and related to protection of individuals regarding the respect for personal data processing and data free flow (FIDALGO, 2019, p. 91). But before being provided through the Proposal, data portability was being debated in other opportunities and initiatives, such as follows: In 2007, the Social Network Users Bill of Rights was enacted, which provided data portability. In sequence, the Data Transfer Project was initiated, having adhered Google, Facebook, Microsoft, LinkedIn, among others (BOZDAG, s.d.)

storage and use, appears as a tool of empowerment. With data portability, the data subjects feel more stimulated to use their data and to migrate freely between different services, even choosing the ones that have the policies that suit their interests the best.

In addition, data portability also seeks to promote competition in a market known for monopolies and network effects by reducing switching costs and the lock-in effect[3]. Thus, personal data portability is not only desirable but needed in a digital reality.

However, innumerable doubts arise regarding data portability implementation[4] and its peculiarities. In this sense, the paper aims to analyze the most critical points of data portability in the Brazilian context based on comparisons of other legal systems, especially the experience of the European Union.

2. Legal nature of personal data portability

There was, in the scope of the European Union, a discussion about the right to data portability's true nature, which initiated even before the Regulation's approval when it was only a project. The debates included doubts about the relevance and the affinity of this legal concept to data protection. There were stances that advocated that data portability was something strange and external to privacy protection (GOLA, 2018).

Indeed, in a preliminary approach, it could be thought that data portability would be a legal concept closer to consumer or competition law.

[3] Besides these costs and effect "it is certain that misinformation of the common user and the convenience of the adhesion to the big web platforms are factors that initiate power agglutination by indiscriminate data collection." (MARTINS; FALEIROS JÚNIOR, 2020, p. 219.)

[4] A recurring concern in matter of data portability is related to compliance costs, which can be a burden too large for small companies. According to Carolina Banda, the big companies could be willing to develop softwares to respond to data portability. On the other hand, to small businesses and startups the efforts are considerable, even having the possibility to be presented as a barrier to market entry. (BANDA, 2016/17.)

However, the acknowledgement of data usefulness and its use by data subjects depends on the evolution of society itself, as well as on larger digital awareness and education of data subjects. Companies had already noted, a long time ago, that data is useful to craft more customized services and to meet more effectively the consumer's standards.

Data is also an important input to individuals, subsidizing and guiding the development of their personal faculties, achievements and satisfactions. When recognizing the value of data also as an input to individuals and not only to organizations, but data portability can also be used as a management and facilitation tool in the personal decision-making process.

For instance, it can help us verify the impact in our consumption patterns and to adopt more sustainable habits, among other possibilities. An example would be the transfer of our shopping list to a nutritional advice app or the use of our data on transportation and power consumption to create a personal carbon index[5].

To the Government, data portability can be used to enable debureaucratization. Besides, it is a tool that will enable legitimately a secondary use (reuse) to data and according to the data subject's expectations[6].

Therefore, data portability needs to be understood as a tool for promoting redistribution of power and benefits of a reality powered by data, generating value for data subjects. It is a user-centered tool that enables data subject agency in the data ecosystem (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 4)[7].

---

[5] In this regard, see: https://www.latribune.fr/opinions/la-portabilite-des-donnees-un-levier-citoyen-pour-la-transition-ecologique-854175.html

[6] In the scope of the European Union, the Commission enacted a Directive proposal to promote governmental data reuse: EUROPEAN COMMISSION, 2018.

7 Data portability can also be understood as a new-generation right (MONTELEONE, 2017, p. 202.)

Thus, it is impossible not to recognize that data portability, apart from its potential effects on the market and on consumer welfare, is an individual (GERADIN; KUSCHEWSKY, 2013) right of each data subject that enables a larger data management and control (in a sense of deciding who will access and maintain its data). This right, furthermore, is not limited to data transfer between service providers (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 3), on contrary, it can be exercised by mere obtention of a copy by the data subject for personal use.

Data portability has also been understood as a mere data transfer, without terminating the relationship. Therefore, data portability solidifies the advance of a new generation of data protection laws, taking a step further, as traditional mechanisms of access, rectification, cancellation and resistance are no longer sufficient to guarantee adequate protection (KESSLER; DRESCH, 2020, p. 23) and informational self-determination.

Besides featuring a personal data protection evolution, data portability has also technical implications on other areas. In this sense, data portability can enable the creation of datasets and the access to data, an important element for developing new technologies and artificial intelligence[8-9-10].

Still, data portability can be an important tool for promoting society's collective or diffuse interests. The citizens can request that their data stays available in the future when an enforcement of a public policy or a scientific mission could publicly call for data (VILLANI, 2018, p. 30).

[8] Data access for the development and implementation of Artificial Intelligence is fundamental (EUROPEAN COMISSION, s.d.)

[9] Despite data usually being "free', non-exclusive and non-rival, the access to it is still difficult. This restriction stems from the data collection, storage and distribution's infrastructure. Besides technological barriers, there are also legal and behavioral barriers (LUNDQVIST, 2018.)

[10] It is mentioned the indispensable need to transfer and to exchange data among business and sectors for developing the Internet of Things (GRAEF *et al.*, 2019, p. 23.)

For these reasons, data portability must be stimulated and promoted, even when related to other regulatory policies[11], to cover other data rather than only personal data[12], especially because of the difficult distinction, in practice, between personal and non-personal data (GRAEF*et al.*, 2018). However, it is necessary clarity and conceptual delimitation on some essential topics of data portability, namely, to guarantee safety and respect for other important values in terms of data protection[13].

3. Data portability as provided through the Brazilian Act (LGPD)

The right to data portability was not provided by all general data protection bills[14]. Among the active bills in the legislative process, only the PL - Bill - 5.276/2016 has brought data portability as a data subject right (BIONI, 2015, p. 57), in its article 18, item V.

In 2018, the PL 4.060/2012 was analyzed by the Chamber of Deputies, being appended to the main bill the PL 5.276/2016 and the PL 6.291/16. A substitute project was approved, which provided the right to data portability.

In sequence, the bill was passed in the Senate and sent to the President for signing. On the 14th of August 2018, with partial veto, the Lei

[11] In this regard, we highlight the initiatives related to Open Banking. See HOFFMANN, 2020, p. 40.

[12] An example is the legal provision provided by the article 6th of the Regulation (EU) nº 2018/1807,
which deals with the regime for the free flow of non-personal data in the European Union.

[13] Besides criticism related to safety and data portability implementation difficulties, especially for small companies, there is also criticism being made by some North American legal scholars, according to Laura Drechsler, that data portability reinforces the idea of data as property. When treating data as a personal asset, data portability could raise complex issues on property and ownership (DRECHSLER, 2018, p. 12.)

[14] According to Paula Ponce, in the writings of the first stage of the public consultation for the crafting of the Personal Data Protection bill, promoted by the Ministry of Justice and ended in April 2011, there was no mention of right to data portability. This right was inserted only in 2015. (PONCE, 2020.)

Ordinária n. 13.709/2018, named Lei Geral de Proteção de Dados Pessoais (LGPD) was enacted, providing the right to data portability in its article 18, item V, of the LGPD[15].

With little provisions about the right to data portability, the LGPD was extremely brief limiting itself to provide that (i) data portability will be performed among data providers, upon express requisition, according to the national authority provided regulation, respecting trade secrets (item V)[16]; (ii) data portability does not include anonymous data (art. 18, § - paragraph -7th); (iii) the national authority will provide the interoperability standards for the purpose of data portability (art. 40); and (iv) health data sharing among sensible personal data controllers is forbidden, except, among other exceptions, to enable data portability when requested by the data subject (§4th, item I, art. 11)[17].

Besides these specific provisions on data portability, when exercising this right, the §3rd of the article 18, that provides the need of an express request from the data subject or from its legal representative to the data processing agent, will have to be followed (note that the law refers itself to the personal data processing agent that can be the data controller or the data operator, which is the one who performs personal data processing in the name of the data controller).

There is also legal applicability of the §4th of the same article to data portability, that provides in case of impossibility of immediate adoption of the provided through the §3rd of this article the data controller could: (i)

[15] With the Law 13.853/2019, that converted the Provisional Decree n. º 859/2018, the writing of the item V, of the article 18, ended up being modified a little to displace the expression "observed the commercial and industrial secrets" to the end of the phrase. It is accepted that the modification was positive, since with the new writing there will be no doubts that the regulamentation will be on data portability and not on the matter of trade secrets.

[16] Such a legal provision implies that data transfer will be directly among data controllers.

[17] Despite the mention made through the LGPD about data portability related to data sharing of sensible health data, "data sharing" cannot be confused with data portability because that can occur even without the data subject's consent, if there is legal ground. (VIOLA; HERINGER, 2020.)

communicate that it is not the data processing agent and point, when possible, the agent; (ii) indicate legal or non-legal reasons as to why it cannot adopt immediately the provision. Still, the §5th of the aforementioned article mentions that the requisition will be complied without cost for the data subject[18], on terms provided through the regulation which is also applicable to data portability.

At last, there are the provisions of §1st and §8th of the article 18 which provide data subject the right to petition to the National Authority or to consumer protection entities (art. 18, §1st and §8th, LGPD) (BERGSTEIN, 2019, p. 2). Therefore, if the data subject has its right to data portability denied or hindered by the data controller, it can turn to the competent authorities, safeguarding its access to justice.

Ultimately, despite the aforementioned legal provisions, the lack of legal provisions on this right creates innumerable doubts about its content, extent and applicability to data portability. Thus, in the next topics, it is shown some interpretative proposals about data portability in Brazil, in light of comparative law (in particular the GDPR).

4. The Definition of Data Portability

Data portability is a global tendency that embraces various distinct initiatives[19]. As Peter Swire (2020, p. 2) points, these initiatives revolve around the following perspectives: (1) data portability as an individual right, provided by legislation such as the GDPR, (2) debate about regulation of large platforms and (3) regulations of different data transfer sectors.

[18] As Ana Frazão highlights: "the right to data portability, to reach such goals, must be easy, free and granted in a way to enable data use with efficiency and safety". (FRAZÃO, 2018). Furthermore, there is a stance that the data subject does not need to show a motive to exercise its right to data portability.

[19] Peter Swire prefers the term "portability" for an individual's data transfer and the expression "other required transfers" for data transfer between two or more people. And the term "PORT" for the *genus* which include these two species. (SWIRE, 2020, p. 2.)

When it comes to data portability as an individual right, comparing the LGPD to other legislation, it is possible to verify that there is no common definition for data portability. In the European scope, we have the article 20 of the European General Data Protection Regulation (GDPR) which has to be interpreted in light of the Recital 68.

This article provides that "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided". The same article still provides that the data subject also has the right to have this data transmitted between the entity responsible for the data processing, whenever technically possible.

In the United States of America, California Consumer Privacy Act (CCPA) provides that the consumer must receive their data in a portable and readily usable format that allows the transmission of this data to third parties. The CCPA provides that this must be done only when technically feasible.

The fact is that each legislation has defined the right to data portability in a diverse way[20]. Some focus on the right to a direct data transfer to a new data controller, others focus on the right to receive and to store data into some personal device or the data subject's right to send data to the new data controller.

In Brazil, we propose a broad concept to data portability, that can be defined as the data subject's right (i) to receive personal data concerning to it in a digital format for use and/or storage from the data controller; (ii) to transfer this data to another data controller, in the present or in the future;

[20] Based on the Swiss Code of Obligations, which provides in its article 400, par. 1, the obligation to give back everything that was received during a contract, it is possible to advocate for a right to data portability for consumers, according to Alberini and Bemhamou. (ALBERINI; BENHAMOU, 2017)

and (iii) to request that its personal data be transferred directly to another data controller (receiver) when technically possible[21].

Note that the first two cases (i) and (ii) already find legal grounds in Brazil, despite finding it in the right of access, as visualized in the §3rd of article 19 of the LGPD. Thus, these two ways of exercising the right to data portability can be requested by the data subject, as well as the case (iii), provided through the data portability's item itself (art. 18, item V, of the LGPD).

It is up to reflection, however, if this division of data portability (the first two cases covered through the right of access and the third case through the right to data portability itself) by the legislator was the right decision because it seems to exist some sort of mismatch and disharmony between what was provided through the item V of the article 18 that does not limit data portability to the data processing based on consent or on a contract, and what was provided through the §3rd of the article 19 of the LGPD. Precisely to avoid this fragmentation, it is understood that these ways of exercising the right to data portability itself (data copy /transfer to another data controller) should be a question of portability, as provided through the GDPR, in its article 20 (n. º 1 and n. º 2)[22].

Another important topic is the direct data transfer to another data controller (art.18, item V). It is understood that this way of exercising the right to data portability does not imply, by itself, the termination of the relationship between data subject and data controller (sender), except when the data subject desires so.

There are cases that the data subject will want only to use its data in another service which sometimes is not even a direct competitor to the data

[21] It is defended that the expression "technically possible" should not be interpreted in a broad manner because the direct data transfer among data controllers is the most effective form of data portability in terms of positive effect on society and the market. (GRAEF *et al.*, 2017, p. 23.)

[22] In the European Regulation's scope, the right of access is different from the right to portability, since the first does not enable data reuse.

controller, but a mere complimentary service. For example, the already recurrent use of API (Application Programming Interface)[23-24-25] for data transfer, as it is the case of social logins.

The APIs are a set of protocols that define how software components communicate with each other. When enabling a company to easily access data generated by other companies, it is possible to catch a glimpse of the development of an interoperability between different agents(BORGOGNO; COLANGELO, 2018).

Besides APIs, the stimulus to develop the Personal Management Information Systems (PIMSS) is important, which will have a crucial role if data portability is to be widely implemented. The PIMSS enable facilitation for the complex consent management system and offer users a dashboard to monitor its data use. The PIMSS work as a data controller, with direct exchange between external data controllers[26] . (CENTRE ON REGULATION IN EUROPE (CERRE), s.d.)

Note, then, that there will be cases in which the data subject wants to remain in the service, requesting only that its data be "duplicated' and sent to another data controller. See that a peculiar aspect about the digital market is that consumers, frequently, want to use various platforms at the same time (multihoming), which is possible by exercising the right to

[23] The use of standardized APIs would enable a continuous portability, according to the Centre on Regulation in Europe. (CENTRE ON REGULATION IN EUROPE (CERRE), s.d.)
[24] The European Data Protection Supervisor also understands that development of standardized APIs must be incentivized. (EUROPEAN DATA PROTECTION SUPERVISOR, 2020)
[25] In the SynchroniCity's guide, which is based on the OASC Minimal Interoperability Mechanism principles (MIMs), there is emphasis on API use for data storage and access as an essential element for the possibility of reapplication and portability of models of technologies to various different cities and communities, and that can be an important orientation for developing Smart Cities. See: SYNCHRONICITY, s.d.
[26] The creation of tactic solutions for PIMSS promotion is highlighted in the document elaborated by the Helsinki EU Office. (HELSINKI EU OFFICE, s.d.)

personal data portability (ENGELS, 2016). It is the possibility to establish a "second digital home" for the data subject (FIDALGO, 2019)[27].

It is observed, furthermore, that the exercise of the right to data portability does not imply the termination of the relationship between data subject and the data controller (sender), except when desired so by the data subject[28]. In this case, the exercise of the right to data portability will imply the termination of the data processing after its transfer, the reason why it could be called "data portability *stricto sensu*".

Lastly, the article 16 of the LGPD enables data preservation, even after the termination of the data processing, for the purpose of data transfer (item III of the mentioned article). That is, even after the data transfer for the purpose of data portability, there may be data preservation, if there is present any case provided through the items of the article 16, such as the need to comply with a legal obligation, or even so if the data subject wants to continue its relationship with the data controller. Therefore, in case the data subject only transmits its data (in the case of multihoming use), the data portability will not imply the erasure or the elimination of data (KESSLER; DRESCH, 2020, p. 37).

However, in case the data subject wants to use data portability to migrate to another service, terminating the relationship with the sending data controller, it is important to verify, in the concrete case, if there is legal ground to continue data processing by the sending data controller (originary). This because, despite data portability not being a case for termination as provided through the article 15 (KESSLER; DRESCH, 2020, p. 49), if the data subject wants to terminate the relationship with that data

[27] As well observed by Vitor Fidalgo, in the GDPR scope, there are no provisions about data elimination (article 17 of the GDPR) on data portability. (FIDALGO, 2019, p. 119.)

[28] As a rule, there is no termination of the data processing by simply exercising the right to data portability, except when it is the data subject's intention on terminating the relationship (data portability *stricto sensu*) and on eliminating data or if it is present any cases of termination of data processing (article 15 of the LGPD)

controller, it could be a case of consent revocation or end of processing (item I and III).

5. The difference between right to data portability and right of access

During the GDPR's legislative process, it was advocated the possibility to add the right to data portability in the right of access. It was not the accepted option on the final Regulation's text, ending up consecrating data portability as an autonomous right and distinct from the right of access (FIDALGO, 2019, p. 91).

The right to data portability, therefore, can be seen as a step forward, an evolution in light of the right of access, as the data format would no longer be limited to what was chosen by the data controller, besides enabling data reuse (DUARTE; GUSEINOV, 2019, p. 110) by the data subject itself or by another data controller. It is a novelty brought through the GDPR, since the former Directive 95/46/EC had not brought such modern right[29].

Another difference between right of access and right to data portability in the European scope is their limit and applicability. Data portability includes only data provided by the data subject and only when the data processing is automated and consent-based or based on a contract execution (GRAEF *et al.*, 2017, p. 1367). Such restrictions and limitations, however, do not apply to the right of access as provided through the GDPR so that the right of access and the right to data portability end up complementing each other (STIFTUNG DATENSCHUTZ, s.d.).

In Brazil, there was no clear distinction between right to data portability and right of access as happened in Europe. Some aspects of the

[29] It is worth to point, however, that the Directive 95/45/EC already provided the right of access.

GDPR that appear in the right to data portability were provided through the LGPD in the right of access, as can be seen through the §3rd of the article 19 of the LGPD.

As already mentioned, the reflection about the correctness of the Brazilian legislator's choice is valid because it seems to exist some sort of mismatch and disharmony between what was provided through the item V of the article 18 that does not limit data portability to the data processing based on consent or on a contract, and what was provided through the §3rd of the article 19 of the LGPD. Furthermore, in Brazil, it was given the data subject a choice on how the right of access was granted, if by digital format or by printed format (art. 19, §2nd, of the LGPD).

6. Data Processing Covered through Data Portability

In regard to the extent of the right to data portability, it can be said that it is applied, as provided through the article 3rd of the LGPD, to a natural person in any data processing operation performed by natural or legal, private or public, person, independently of where it is its headquarters or in what country the data is located, as long as (i) the data processing operation is performed on national territory, (ii) the processing has the purpose of offering or providing goods and services or data processing of individuals located on national territory, or (iii) the personal data object of processing has been collected on national territory.

However, the right of data portability is not applied to, since excluded from the provisions of the Law No 13.709/2018 (art. 4th), data processing (i) performed by a natural person solely for private purposes; (ii) performed solely for journalistic, artistic or scholarly purposes; (iii) performed solely for public safety, national defense, State security or criminal investigation and criminal offenses repression purposes; or (iv) from outside the national

territory, as provided through the item IV of the article 4th of the Law No 13.709/2018.

7. Covered Data

In the same way as the GDPR (Recital number 26), anonymous data is not covered by data portability as provided through the §7th of the article 18 of the Law 13.709/2018. However, it is advocated that whenever it is possible to identify the data subject by providing additional information, such data must be covered by data portability, as it has been defended in Europe, with legal grounds on the article 11 of the Regulation (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, s.d.). Pseudonymised data shall, then, be covered by data portability.

In relation to the kind of data covered (provided, observed and inferred), there is no specific definition in the LGPD. In the GDPR's scope, data portability has been limited to provided data, which represents a significant change in the final text compared to the initial bill (HERT *et al.*, 2017)[30].

It is understood that it is necessary a larger reflection when it comes to the absence of a specific definition in the item V of the article 18. It remains controversial still if such absence could be considered an eloquent silence of the legislator to cover other "treated data" (that is, provided, observed and inferred) [31], or if such definition was reserved to regulamentation.

[30] It is understood that provided data is also covered as is the case of observed data. Data profiling, then, would not be covered through data portability provided through the GDPR. However, companies could voluntarily promote this kind of data portability, as a sign of accordance and trust. (U VRABEC, 2018)

[31] As said by Paula Ponce, such a question was debated in Congress, when the Provisional Decree nº 869/2018 was being appreciated. The proposal of the Amendment nº 42 had the purpose of excluding data derived from data portability. However, the amendment was rejected by the Commission, which understood that data portability would relate only to data provided by the data subject itself and not that generated or complemented by the data controller. (PONCE, 2020.)

In Singapore (SINGAPORE, 2020), the Personal Data Protection Commission has proposed a public consultation for the purpose of defining the implementation of data portability. One of the topics of consultation was the kind of data that data portability would cover.

In this consultation, the Singapore Commission proposed the application of data portability to data generated in digital format that is (a) provided by the individual and (b) generated by the user's activities. After feedback, the Commission expressed interest in keeping this scope, but it intends to emit a white-listed dataset that specifies a pattern which data must be subjected to data portability to guarantee more clarity and certainty for organizations.

8. Legal Grounds

In the GDPR, data portability was limited to data processing performed on a consent basis or needed for the contract execution (Recital 68 and article 20, n. 1, point "a"). Besides that, it is necessary that it was performed in an automated manner, that is, in a digital format (article 20, n. 1, point "b").

In the LGPD, the right to data portability did not suffer any limitations related to legal grounds (there was only a restriction on the right of access, as provided through the §3rd of the article 19). However, it is understood that a broad data portability coverage could backfire, precisely because of compliance costs. Therefore, the reflection about the possibility of such a question being covered through the Brazilian Data Protection Authority (ANPD) regulation's is brought.

9. Coverage - Subjective Aspect

A literal reading of the article 18, item V, of the LGPD, could lead to the conclusion that data portability would only be applied to data controllers

when they fit the concept of "data provider". And to define such a concept it would be necessary to dialogue with the Brazilian Consumer Protection Code (CDC)[32-33].

On the topic, it is understood that the LGPD has not used the best technique when using the expression "provider" in the item V of the article 18, especially because such a concept creates legal fragmentation going against the objective of a general law: to guarantee legal uniformity and certainty. Moreover, the caput of the article 18 itself provides the data controller as the entity responsible for promoting data subject rights, which should also be applied to data portability, since topographically inserted in this article.

Still, considering that data portability is an individual right, not limited to the promotion of the consumer and competition welfare, the LGPD should not have made such a legal outline. As seen before, data portability has an intimate relation with informational self-determination, reason to why it should be applied broadly to data processing and not only to data generated due to a consumer relationship. Employment relationships are an example of data portability being important and useful to the data subject.

10. Interoperability

[32] In relation to data portability application to the Government, a literal interpretation of the item V, article 18 of the LGPD, the Government could only be obligated to assure data portability when it plays the role of provider, according to the article third of the Consumer Law. Generally, with exception to public companies and to mixed capital companies that operate with economic activities in the strict sense, the Government is considered a provider when it provides public services that are singular and fee based. In this case, data portability would be applied almost "exceptionally" to the Government, since most of its activities do not fit the aforementioned characteristics.

[33] In Europe, the GDPR in its Recital 68 expressly says that, by its nature itself, data portability should not be exercised in relation to the entity responsible for personal data processing when it comes to the pursuit of its public duties or the exercising of its public authority. That is, in the Government, its application will be extremely rare, only when operating on a contract or a consent basis; However, data portability can be adopted as a good practice by the public sector in other cases. (EUROPEAN COMMISSION, 2018, p. 7.)

Before the legal texts analysis (GDPR and LGPD) to inquire what they provide about interoperability, it is necessary to differentiate the concepts of "interoperable format" and of "interoperability". Interoperable format would be minimum patterns for ensuring the possibility of data exchange and reuse (EUROPEAN COMMISSION, 2018), as it is the following set: structured format, commonly used and machine-readable (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 17).

An interoperable system or the interoperability, however, are related to the capability of communication, to program execution or to data transfer between distinct functional units, without needing to know exclusive characteristics of each unit (PUCCINELLI, 2017, p. 207). The thematic of an interoperable system is covered through the ISO/IEC 2382–01.

In Brazil, in the Federal Government (BRASIL, 2012), there are various initiatives for development of interoperability for purposes of implementation of digital governance policies. In the Interoperability Guide, as well as in the Decree nº 10.046/2019[34], interoperability appears as the capability of various systems and organizations working together.

In Europe, the European Parliament and Council's Decision nº 992/2009/EC defines in its article 2nd, point "a", the interoperability as the capability of disparate and diverse organizations to interact upon data interchange among the related systems.

In the LGPD, the Law itself makes it possible, in its article 40, that the national authority provides interoperability patterns for the purpose of data portability. Since, until the enactment of a regulation in Brazil, there is no need for interoperability between services. Thus, if technical barriers appear when performing data portability (namely the case of a direct data transfer to another data controller), the data controller must explain these

[34] It is worth pondering that despite the objective of combating fraud and management efficiency pursued through the Decree 10.046/2019, some criticism is made towards the Decree, precisely in light of the lack of safeguards and ways of control by the citizen of how its data will be treated and by which entities. (MARANHÃO; CAMPOS, 2019)

barriers in an intelligible and clear manner for the requesting party (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, s.d.), considering the §4th of the article 18 of the Law.

However, despite the interoperability for the purpose of data portability not being obligatory in Brazil yet, it is advocated that when indeed performed the data controller use interoperable formats to enable data reuse. Note that the LGDP has not brought any requirement as to what data format must be used, but based on a teleological interpretation it is possible to reach this conclusion, since without the use of an interoperable format data portability might not bring any benefit for the data subject, precisely because of the difficulty of data reuse (COLOMBO; GOULART, 2020, p. 94).

It is stressed that there is already a provision in our legal system related to interoperable data format. The Decree n. 8.771/2016, which regulates the Civil Rights Framework of the Internet Act, in its article 15, establishes that data must be kept on an interoperable and structured format to facilitate access due to a judicial ruling or a legal provision. Also, the article 25 of the LGPD provides that: "The data must be kept in an interoperable and structured format for data sharing related to public policies execution, public services provision, Government decentralization and dissemination and access to information for the general public".

Thus, it is concluded that in Brazil there is no requirement of interoperability for the purpose of data portability so far, despite the possibility of being eventually provided through the Brazilian Data Protection Authority (ANPD)[35], as provided through the article 40 of the LGPD. Such a conclusion does not take back the requirement of compliance

[35] The responsibility, however, when it comes to the promotion of interoperability does not need to be limited to the ANPD (Brazilian data protection authority) so that in the regulated sector it is possible that the promotion could be done by other regulatory authorities (for example what is happening with the Open Banking). Moreover, the market itself can take center stage in the development of interoperability through good practices, in light of the article 50 of the LGDP.

to an interoperable format so that is, at least, structured in a current use and automated reading.

In Europe, it is understood that for compliance to data portability purposes, the entity responsible for data processing must provide personal data in an interoperable, structured, of current use and of automated reading format (Recital 68 of the GDPR). However, even if interoperability is desirable (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 17), there is no obligation to comply with it[36], as provided through the Recital 68: The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".

It is worth noticing that in the original writings of the GDPR, it was assigned to the Commission the role of identifying a common transfer format. However, such a necessity to define a format ended up being abandoned, precisely because of the existing divergences and discussions about the competitive implications of imposing a format (MONTELEONE, 2017, P. 209).

Despite not existing an obligation of interoperability, Paul Hert *et al.* (2017) suggest that it should be required. According to the authors, the Regulation's true intention would not be a mere direct data transfer between a data controller and another one but a development of a solid interconnection between different digital services, promoting, then, a user-centered system.

This stimulus for compatibility and for interoperability is not new and can be found in recent jurisprudence in the United States of America, as in the Lotus Development Corp v Borland International case (UNITED STATES OF AMERICA, 1995), quoted by Peter Swire and Yianni Lagos (2013). In this case, the Court ruled that the Lotus company could not use

[36] Note that in case of a direct data transfer (article 20, n. 2 of the GDPR), the text itself provides that it will only be perform when technically possible.

its copyright protection to prevent the creation of competitor softwares that enabled interoperability.

In the European Union, there is a similar provision to the North American precedent's one. It is the Computer Programs Directive of 1991, which provides the exception to the copyright, enabling third-party companies to observe, study and copy a program of another company when needed to reach program interoperability.

Interoperability can be produced on complimentary markets, which will have a stimulus to develop it or even have the possibility to come up originally. Given this, it would be possible for the intellectual property rights concession to promote an even better experience in terms of data portability in a similar way to the North American and European aforementioned precedents.

It has been understood that without interoperability is very probable that data portability does not come to generate all of its potential effects[37]. Maurizio Borghi ponders that the pro-competition effects of data portability end up being more pronounced in markets with common data processing systems than in the ones with no interoperable patterns (BORGHI, 2019, p. 15).

11. Data Portability and Third-Party Rights

It is still possible that the right to data portability to conflict with other rights[38], such as that of trade secrets or intellectual property rights protection. Another problem that could arise is related to third party privacy

[37] The recent OECD report "Going Digital in Brazil" highlights the importance of developing interoperability patterns for data portability purposes. (OECD, 2020, p. 199.)
[38] As Indra Spiecker points out, until there is not a creation of a standardized information right that strikes an appropriate balance between interests, the right to data protection will collide several times with other rights. (SPIECKER, 2018)

rights[39] when, for example, a person wants to port a photo in which other people appear. (SWIRE; LAGOS, 2013, p. 349)

In these cases, it is possible to bring up the provisions of item II, of the §4th of the article 18 of the LGPD, considering a legal reason that prevents adoption of data portability. There is also expressed legal reservations provided by item V of the article 18 which provides that data portability will respect trade secrets[40].

In Europe, the article 20, n. 4, expressly provides that data portability cannot harm third party rights and freedom. On the same line, the Recital 68 warns: "Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation".

It is worth noting the application of these reservations, be it provided through the article 20, n. 4, of the GDPR, be it through the item II, of the §4º of the article 18 of the LGPD, should not happen in any case of possible harm to third party rights but when data portability affect them adversely, that is, in an unjustified or illegitimate way. This needs, thus, a case-by-case approach (HERT *et al.*, 2017).

According to the Data Protection Working Party of Article 29 (Art. 29 WP), in various opportunities data controllers will end up treating data related to different data subjects. But this fact should not be used to deny or to restrict data portability. What must be observed is that the new data controller, if there are no legal grounds for such, must not treat third party data when it could harm these third-party subjects (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 11-12).

[39] This question is also brought up in the White Paper published by Facebook. (FACEBOOK, 2019.)

[40] The LGPD does not define how or in what grade this interest must be respected, neither conceptualizes what can be considered as trade secret.

Thereby, the Art. 29 WP (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 11-12) suggests in order to avoid adverse effects to third party subjects involved that such personal data processing performed by another data controller is possible only when data is maintained under exclusive control through requesting data subject and managed only for purely personal or domestic needs. That is, if there are no legal grounds, the new data controller cannot use third party data for its activities, such as that of profile or statistics enrichment or marketing targeting.

Another interesting tool suggested by Art.29 WP is that before executing data portability data subjects should be enabled to select which data they want to transfer. With this solution, the data subject itself can already leave third party data out. It is also possible to promote the search for third party consent to legitimate data transfer (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 11-12).

Among third party rights, there are also trade secrets and intellectual property rights. Such a conclusion can also be obtained through analogical interpretation of the Recital 63 of the GDPR. In Brazil, the trade secret was expressly provided through the item V, article 18, of the LGPD, and this will be further analyzed with more details.

Regarding the possible conflict between intellectual property rights and data portability, Vítor Fidalgo (2019, p. 125) says that this problem is more seeming than real because: in relation to raw data, the execution of data portability will not be an illegal use of a software or database. In the case of software, the attributed protection concerns only its expression, in a way that data portability would not violate this right. Regarding the database, it could be decompiled before sending. Lastly, in relation to the creator of the database, data portability does not represent a substantial violation if considered that it will only be transferred as part of the database's content, which may not even be quantitatively significant.

12. Trade Secret

In the LGPD's text, we can find about thirteen provisions on the need to observe trade secrets[41-42]. Despite the legislator's large concern with trade secret protection in the scope of personal data protection, this is one of the more neglected and less studied subject-matters in Brazil (PELA, 2018, p. 546), not existing a precise definition about its content, besides being conditioned to unfair competition practices.

As a matter of fact, the LGPD provisions on trade secrets have to be applied with caution, be it because of the lack of tradition or consensus on the subject, be it because of the lack of interpretative vectors in the LGPD, which does not define what can be considered as a secret not even to what measure or grade of interest must be observed.

It needs to be reflected specially upon how it will be harmonized the intangible information monopoly generally protected by trade secret with the rights granted for data subjects on data access, use and processing (MALGIERI, 2016).

Independent of the choices being made related to the intensity given to trade secret protection, especially when conflicting with data subject rights[43], it must be pondered that a mere obtaining of a personal data copy for private use or the right to access by the data subject does not have, *prima facie*, the capability of generating losses on competition in an unfair

[41] The provisions on trade secrets were brought through the Plenary Amendment 9, received in the Plenary during the Bill 4060/2012's appreciation by the Brazilian Chamber of Deputies, being attached to the main proposal the PL 5.276/2016 and the PL 6.291/16

[42] There is a myriad of words in Brazil to designate the confidential data of companies that deserve legal protection (FEKETE, 2003, p. 17). Given that the expression "trade secret" is a *genus* that ends up covering the other species, such as that of commercial and industrial secrets (BARBOSA, 2013, p. 124), it was opted to use the *genus* "trade secret" in this article.

[43] It must be noted that the right to data portability is the right, among others of the LGPD, to have the most implications on unfair competition, subject-matter that regulates trade secrets in our legal system.

way to the company (and the trade secret protection in Brazil is conditioned to an act of unfair competition).

Another important topic related to trade secret is data inference, which is obtained by raw data processing, performed generally by artificial intelligence. This data inference points the preferences, tastes and conditions of a certain person. It is also considered as data inference the creation of profiles and rating systems.

As being crafted by companies through investments and technologies, could data inference be protected by trade secret rights? Answering this question is no easy task, especially because it would be necessary to research thoroughly the legal nature of data inference as to verify if it is considered personal data.

Anyway, it is possible to ponder that, if the information generated by data processing is no longer associated with the original data, so that the data subject could no longer be identified, making it impossible to backtrace, it can be protected by trade secret rights. Furthermore, the techniques and the algorithms used to obtain information and knowledge can also be covered by trade secret rights (WACHTER; MITTELSTADT, 2019, p. 79)[44].

13. Civil Liability Regime for Data Portability

The implementation of data portability brings innumerable challenges and there is no simple solution. One of the data controllers main concerns is how to promote data portability safely and without jeopardizing the protection of data subjects itself[45]. With such a concern comes the inquiry about eventual liability of the data sender and data receiver[46].

[44] However, there is the possibility of mitigating the algorithm's protection in favor of the data subject. For example, the metamorphic algorithms, which as they process personal data, they end up modifying themselves.
[45] The safety subject is one of the main topics covered by the recent FTC's workshop (https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability).
[46] For a deeper analysis, see: CRAVO *et al*., 2020, p. 185-202.)

On this path, a characteristic of data portability that deserves more attention concerns the risks for privacy that may arise from it. From the moment that data has become completely portable, it is easy to evade any privacy policies of the original data provider, to whom it was requested.

As a matter of fact, it would be enough transferring data to a new platform for the old legislation and policies to be no longer needed to be followed (YOO, 2012, p. 1155). Besides, there could be frauds in the identification of users that would enable an offender to port data among different platforms (ENGELS, 2016) or even to obtain a copy of it.

Thus, to reap all of the benefits of portability, it is indispensable and urgent that the liability and the legal duties to be observed are established very clearly (UNITED KINGDOM, s.d.). Well, in this attempt to define the civil liability regime of data portability, it should be taken into account, as a premise, the responsibility regime provided through the arts. 42 to 45 of the LGPD.

Therefore, for purposes of civil liability it is needed the breach of a duty, be it specific or general. When it comes to legal duties related to data portability, besides the general duty of safety, it is possible to identify specific duties in each step of data portability, which are: 1) data portability requisition, 2) pre-transfer, 3) transfer and 4) post-transfer (CRAVO *et al.*, 2020).

The first step of requesting data portability is one of the most sensitive since it will be necessary to verify if the one who requests data portability is, indeed, the data subject. It is important, therefore, to steer clear of unnecessary personal data collection. Still, it is necessary to avoid frauds of malicious people.

A possibility is the use of two-step verification or the requisition for the requesting party to enter its password. Still, it can be sent an email to the address of the requesting party register for confirmation if it really wants to proceed with that requisition (and even prevent the transfer in

case the data subject does not recognize that requisition (FACEBOOK, 2020)).

From the experience of the GDPR, it was verified that not always the speed of the answer to the requisitions and the verification of the data subject's identity can be concilied. In this sense, it is worth noting the case of the applicant that obtained data of its fiancée because of requisitions based on the provided rights through the GDPR (HUDDLESTON, s.d.).

In the pre-transfer phase, it arises, already, the question whether the data controller must verify the legitimacy of the receiver. Must the data controller certify that the destination follows policies consistent with data protection? Must it warn the data subject about possible risks?

As provided through the Art. 29 WP, the data sender is not responsible for the recipient's adequacy to the data protection legislation, since it does not participate in the receiver's choice (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016)[47]. A possible solution, pointed by Facebook in the Singapore's Public Consultation, would be the creation of codes of conduct and certifications (SINGAPORE, 2020). When adopting these, the data controller would be safer when performing data portability to another data controller that followed the code or was certified.

In the third phase, data transfer, it must be adopted measures that enable data transfer in a safe way and to the right destination (destination verification measures). Here, the use of adequate formats gains prominence, as well as peer-to-peer encryption (UNITED KINGDOM, s.d.) and new technologies, such as the blockchain (EUROPEAN COMMISSION, 2020).

Maria Viola and Leonardo Heringer highlight that data portability is not consent-based, but on complying with an express requisition. Because of this, the data sender would act more as a mere operator of the activity.

[47] In relation to it, the European Banking Federation issued a statement saying that: "we believe it would be necessary to emphasize that the "sending" data controller cannot prevent adverse effects on any third parties involved in the context of the data portability" (EUROPEAN BANKING FEDERATION, s.d.).

However, this does not remove the responsibility of data sender of checking the operation's safety (VIOLA; HERINGER, 2020, p. 8).

Lastly, in the post-transfer phase, the data sender will not be responsible for data processing done at the destination, even if abusive (VIOLA; HERINGER, 2020, p. 9). Although, the data sender is still responsible for data maintained in their systems (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 9).

The data sender, still, can be hold responsible by sending corrupted data (SINGAPORE, 2020), and it must make sure that data was correctly delivered at the destination (VIOLA; HERINGER, 2020, p. 8). In the condition of new data controller, the data receiver must assure an appropriate legal ground for data processing, be it data of the requesting data subject, be third party data (INFORMATION COMMISSIONER'S OFFICE, s.d.).

14. Final Considerations

At the same time the data portability is one of the largest innovations brought through the GDPR, it also represents one of the largest challenges to the market. Concerns about safety related to data transmission or to interoperability are inevitable, as well as to compliance costs.

As a matter of fact, the apprehension that the observation of data portability could become a burden too large to small companies is inevitable, which will generate a discouragement to market entry or permanence. In the long run, this can generate a concentration of power in the market for big companies, especially if they become APIS developers in order to execute data portability, revealing a possible anti-competitive impact of this tool.

A solution to counterbalance this situation is the adoption in Brazil through the ANPD of clear and precise orientations about the definition and

content of data portability. Still, the stimulus and the promotion of interoperability have become indispensable.

However, this duty does not have to be assigned only to the ANPD. It is possible that the promotion of interoperability could be done also by other regulatory authorities (as an example of what is happening with Open Banking). Furthermore, the market itself could take center stage in the development of interoperability through good practices, in light of article 50 of the LGPD.

Regardless of the choice made in the regulation of the legislation, it is certain that data portability is a data subject right that could be presented in three distinct ways of being exercised, such as: a mere data transfer without terminating the relationship with the data controller, the obtaining a copy of the data in an automated format and data portability *stricto sensu,* with the termination of the relationship and the data subject migration to another service supplier.

Anyway, it must be alerted that any institution related to data portability must be implemented along with safety policies, especially in the data transfer phase. Lastly, it is advocated that the right to data portability must be harmonized with other interests and rights.

Ultimately, if at first glance data portability could be understood only as a mechanism destined for the consumer market, today there is no longer doubt that this right is an individual right of the data subject. Data portability is an evolution that marks a new generation of rights, capable of placing the data subject as the protagonist of the new digital reality.

References

AFUAH, Allan. Are network effects really all about size? The role of structure and conduct. **Strategic Management Journal**, v. 34, p. 257-273, 2013.

ALBERINI, Adrien; BENHAMOU, Yaniv. **Data Portability and Interoperability**: An Issue that Needs to Be Anticipated in Today's It-Driven World. 2017. DOI: http://dx.doi.org/10.2139/ssrn.3038877.

ALSTYNE, Marshall Van. **A platform strategy**: creating new forms of value in the digital age. Capgemini Consulting, 2016.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on the right to data portability**. Brussels: European Commission, 2016.

BANDA, Carolina, **Enforcing Data Portability in the Context of EU Competition Law and the GDPR**. MIPLC Master Thesis Series, 2016/17.

BARBOSA, Denis Borges. **Tratado de Propriedade Intelectual**. Tomo I. Rio de Janeiro: Lumen Juris, 2013.

BERGSTEIN, Laís. Direito à portabilidade na lei geral de proteção de dados. **Revista dos Tribunais**, v.1003, maio 2019.

BIONI, Bruno. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BORGHI, Maurizio. **Data Portability and Regulation of Digital Markets**. CIPPM / Jean Monnet Working Papers, Bournemouth University, 2019.

BORGOGNO, Oscar; COLANGELO, Giuseppe. Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy.**Computer Law & Security Review**, Stanford-Vienna European Union Law Working Paper No. 38, 2018.

BOZDAG, Engin. **Data Portability Under GDPR**: Technical Challenges. Available at: https://ssrn.com/abstract=3111866. Access on the 10th of October 2020.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Guia de Interoperabilidade**: Manual do Gestor / Ministério do Planejamento, Orçamento e Gestão. Brasília: MP, 2012.

CENTRE ON REGULATION IN EUROPE (CERRE). **Making data portability more effective for the digital economy**. Available at: https://www.cerre.eu/sites/cerre/files/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf. Access on the 6th of July 2020.

COLOMBO, Cristiano; GOULART, Guilherme. Direito póstumo à portabilidade de dados pessoais no ciberespaço à luz do Direito brasileiro. In: FLORES, Alfredo de Jesus Dal Molin. (Org.). **Perspectivas do discurso jurídico**: revolução digital e sociedade globalizada.Rio Grande: Editora da Furg, 2020. p. 90-109.

CRAVO, Daniela Copetti.; KESSLER, Daniela Seadi; DRESCH, Rafael de Freitas Valle. Responsabilidade Civil na Portabilidade de Dados. *In*: Nelson Rosenvald; Guilherme Magalhães Martins. (Org.). **Responsabilidade Civil e Novas Tecnologias**.Indaiatuba: Foco, 2020. p. 185-202.

CSERES, Kati J. The impact of consumer protection on competition and competition law the case of deregulated markets. **Amsterdam Center for Law & Economics Working Paper**, n. 05, 2006. p. 4.

DRECHSLER, Laura, Practical Challenges to the Right to Data Portability in the Collaborative Economy. Proceedings of the 14th International Conference on Internet.**Law & Politics**. Universitat Oberta de Catalunya, Barcelona, 21-22 June, 2018.

DUARTE, Diogo Pereira; GUSEINOV, Alexandra. O direito de portabilidade de dados pessoais. *In*: CORDEIRO, Antônio Menezes; OLIVEIRA, Ana Perestrelo; DUARTE, Diogo Pereira Duarte (coord.). **FinTechII**: Novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019.

ENGELS, Bárbara. Data portability among online platforms. **Internet Policy Review**, v. 5, n. 2, 2016.

EUROPEAN BANKING FEDERATION. **Comments to the working party 29 guidelines on the right to data portability**. Available at: https://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.pdf. Access on the 27th of October 2020.

EUROPEAN COMISSION. **DSM cloud stakeholder working groups on cloud switching and cloud security certification**. Available at: https://ec.europa.eu/digital-single-market/en/dsmcloud-stakeholder-working-groups-cloud-switching-and-cloud-security-certification. Access on the 6th of July 2020.

EUROPEAN COMMISSION. **A European strategy for data**. 19 fev. 2020. Available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. Access on the 25th of October 2020.

EUROPEAN COMMISSION. **GDPR Data Portability and Core Vocabularies**, 2018.

EUROPEAN COMMISSION. **Proposal for a Directive on the re-use of public sector information**, 2018.

EUROPEAN DATA PROTECTION SUPERVISOR. **EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust**. 29 jun. 2020. Available at: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf. Access on the 6th of July 2020.

FACEBOOK. **Charting a Way Forward on Data Portability and Privacy**. 04 set. 2019. Available at: https://newsroom.fb.com/news/2019/09/privacy-and-data-portability/. Access on the 27th of September 2019.

FACEBOOK. **Comments to the Federal Trade Commission on Data Portability**. 2020. Available at: https://about.fb.com/wp-content/uploads/2020/08/Facebook-Comments-to-FTC-on-Data Portability.pdf. Access on the 25th of October 2020.

FEKETE, Elisabeth Kasznar. **O regime jurídico do segredo de indústria e comércio no Direito Brasileiro**. Forense: Rio de Janeiro, 2003.

FIDALGO, Vitor Palmela. O direito à portabilidade de dados pessoais. **Revista de Direito e Tecnologia**, v. 1, n. 1, 2019.

FRAZÃO, Ana. Nova LGPD: direito à portabilidade. **Jota**, 07 nov. 2018. Available at: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-a-portabilidade-07112018. Access on the 5th of January 2019.

GERADIN, Damien; KUSCHEWSKY, Monika. **Competition law and personal data**: preliminary thoughts on a complex issue. 13 fev. 2013. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088. Access on the25th of December2017.

GOLA, Peter. **Datenschutz-Grundverordnung VO (EU) 2016/67**. Munich: C.H. Beck, 2018.

GRAEF, Inge, HUSOVEC, Martin, PURTOVA, Nadezhda. Data portability and data control: lessons for an emerging concept in EU law. **German Law Journal 2018**, v. 19 n. 6, p. 1359-1398, 2017.

GRAEF, Inge; GELLERT, Raphael; PURTOVA, Nadezhda; HUSOVEC, Martin*;* **Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data**, 2018.

GRAEF, Inge; HUSOVEC, Martin; VAN DEN BOOM, Jasper. Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes.**TILEC Discussion Paper No. DP 2019-005**, 2019.

HELSINKI EU OFFICE. **Data agile economy from reactive to proactive approach for the benefit of the citizens**. Available at: https://helsinki.eu/wp-content/uploads/2020/05/Data-agileEconomy_From-reactive-to-proactive-approach-for-the-benefit-of-the-citizens.pdf. Access on the 6th of July 2020.

HERT, Paul; PAPAKONSTANTINOU, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. The right to data portability in the GDPR: Towards user-

centric interoperability of digital services. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, p. 1-11, 2017.

HOFFMANN, Jörg. Sector-Specific (Data-) Access Regimes of Competitors. **Max Planck Institute for Innovation & Competition Research Paper** No. 20-08, 2020.

HUDDLESTON, Jennifer. **Comments regarding "Data to Go: An FTC Workshop on Data Portability"**. Disponível em: https://beta.regulations.gov/comment/FTC-2020-0062-0007. Access on the 27th of October 2020.

INFORMATION COMMISSIONER'S OFFICE. **Right to Data Portability**. Available at: https://ico.org.uk/. Access on the 25th of October 2020.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. **Supporting Data Portability in the Cloud Under the GDPR**. Available at: http://alicloud-common.oss-ap-southeast1.aliyuncs.com. Access on the21st of January 2018.

KESSLER, Daniela Seadi; DRESCH, Rafael de Freitas Valle. Direito à Portabilidade de Dados no Contexto Brasileiro e Europeu. *In*: CRAVO, Daniela Copetti; KESSLER, Daniela Seadi; DRESCH, Rafael de Freitas Valle. **Portabilidade de Dados na Lei Geral de Proteção de Dados**. Indaiatuba: Foco, 2020. p. 23-54.

LUNDQVIST, Bjorn. Portability in Datasets under Intellectual Property, Competition Law, and Blockchain. **Stockholm University Research Paper**No. 62, 2018.

MALGIERI, Gianclaudio, Trade Secrets v Personal Data: A Possible Solution for Balancing Rights. **International Data Privacy Law**, v. 6, n. 2, p. 102–116,1 May 2016.

MARANHÃO, Juliano; CAMPOS, Ricardo.**A divisão informacional de poderes e o cadastro base do cidadão**. 18 out. 2019. Available at: https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019. Access on the 22th October 2020.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. O direito à portabilidade de dados pessoais e sua função na efetiva proteção às relações concorrenciais e de consumo. In: LÓSSIO, Claudio Joel Brito; NASCIMENTO, Luciano; TREMEL, Rosangela. (Org.). **Cibernética jurídica**: estudos sobre direito digital.Campina Grande: EDUEPB, 2020. p. 213-228.

MONTELEONE, Andrea Giulia. Il Diritto Alla Portabilità Dei Dati. Tra Diritti Della Persona e Diritti Del Mercato. **LUISS Law Review**, v. 2, 202-2013, 2017.

OECD. **A Caminho da Era Digital no Brasil**.Paris:OECD Publishing, 2020.

PELA, Juliana Krueger. The Brazilian Regulation of Trade Secrets. A proposal for its review. **Gewerblicher Rechtsschutz und Urheberrecht - Internationaler Teil**, v. 6, p. 546-550, 2018.

PONCE, Paula Pedigoni, Direito à portabilidade de dados: entre a proteção de dados e a concorrência.**Revista de Defesa da Concorrência**, v. 8, n. 1, p.134-176, jun. 2020.

PUCCINELLI, Oscar. El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances. **Pensamiento Constitucional**n. 22, p.203-228, 2017.

SINGAPORE. Personal Data Protection Commission. **Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions**. 20 jan. 2020. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations. Access on the 20th of October 2020.

STIFTUNG DATENSCHUTZ. **Practical Implementation of the Right to Data Portability**. Available at:https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/studie-datenportabilitaet.pdf. Access on the 3rd of October 2020.

SWIRE, Peter. **The Portability and Other Required Transfers Impact Assessment**: Assessing Competition, Privacy, Cybersecurity, and Other Considerations, 2020.

SWIRE, Peter; LAGOS, Yianni. Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. **Maryland Law Review**, n. 3, p. 335-380, 2013.

SYNCHRONICITY. **SynchroniCity Guidebook**. Available at: https://synchronicity-iot.eu/wp-content/uploads/2020/01/SynchroniCity-guidebook.pdf. Access on the 26th of September 2020.

U VRABEC, Helena. **Unfolding the New-Born Right to Data Portability**: Four Gateways to Data Subject Control. 23 maio 2018. Available at: https://ssrn.com/abstract=3176820. Access on the 10th of October 2020.

UNITED KINGDOM. **Data Mobility**: the data portability growth opportunity for the UK economy. Available at: https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf. Access on the 25th of October 2020.

VILLANI, Cédric. **For a Meaningful Artificial Intelligence**. Mar. 2018. Available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Access on the 24th of September 2020.

VIOLA, Mario; HERINGER, Leonardo. **A Portabilidade na Lei Geral de Proteção de Dados**. Rio de Janeiro: ITS, 2020.

WACHTER, Sandra; MITTELSTADT, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, 2019.

YOO, Christopher. When antitrust met Facebook. ***G****eorge Mason Law Review, v. 19, n. 5, p. 1147-1162, 2012.*

Artigo recebido em: 11/08/2021.
Aceito para publicação em: 09/11/2022.