UNIVERSIDADE CATÓLICA PORTUGUESA

The guarantee of the data subject rights within data sharing with third parties.

Comparative analyses under the scope of the GDPR and the LED.

Filipa Mota e Costa Moreira da Mota

Master's in law

Faculdade de Direito | Escola do Porto 2020

UNIVERSIDADE CATÓLICA PORTUGUESA

The guarantee of the data subject rights within data sharing with third parties.

Comparative analyses under the scope of the GDPR and the LED.

Filipa Mota e Costa Moreira da Mota
Thesis supervisor: Prof. Dr. Filipa Urbano Calvão

Master's in law

Faculdade de Direito | Escola do Porto 2020

Acknowledgments

Although the thesis is known to be a solitary process, I'm blessed enough to never have felt lonely during this journey.

First, I would like to thank my parents and grandparents for all the love and support given during this time. Always making me smile and warming my heart even when the physical distance separates us.

To Sam, thank you for all the love and caring, to always know how to bring joy to every moment and for supporting me in an immeasurable way.

To Heidi and Nadia, thank you for all the kind words, the constant cheerleading and allowing me to grow with you in a professional and personal way.

To Caio, for all the time given on support and fun during this time.

At last, but definitely not the least, to Professor Filipa Calvão, for a careful and dedicated support and for the sharing of knowledge during all this process. Without them, this would not have been possible.

Abstract

This dissertation sets its objective into the analyze of the data sharing with third parties and the guarantee of the data subject rights in the perspective of the Data Protection Regulation and the Directive 2016/680. In this analyzes the responsible for the data sharing will be a private company and the third parties, the competent authorities, in particular the judicial authorities.

We will start by analyzing, in a comparative perspective, the rights in the regime of the Data Protection Regulation and the Directive 2016/608, in this context we will analyze the data sharing between private companies and the judicial authorities defining which law will regulate, and at what stage, this sharing.

Finally, we will analyze the point of confrontation of the two regimes in the scope of the rights, emphasizing the right of access and the fundamental role that it occupies in this problem.

Keywords: Data sharing; law enforcement authorities; data protection; right of access.

Resumo

A presente dissertação tem como objetivo a análise da partilha de dados com terceiros e a garantia dos direitos na perspectiva do Regulamento de Proteção de Dados e na Diretiva 2016/608. Nesta análise o responsável pela partilha de dados configura a figura da empresa privada e os terceiros, as autoridades competentes, em específico, as autoridades judiciais.

Iremos começar por analisar, numa perspectiva comparada, os direitos no regime do Regulamento de Proteção de Dados e da Diretiva 2016/680, nesse âmbito vamos partir para a análise da partilha de dados entre as empresas privadas e as autoridades judicias definindo qual a lei que regula, e em que fase, esta partilha.

Por último, iremos analisar o ponto de confronto dos dois regimes no âmbito dos direitos desta partilha, dando ênfase ao direito de acesso e ao papel fundamental que ocupa nesta problemática.

Palavras-chave: Partilha de dados; autoridades judicias; proteção de dados; direito de acesso.

Table of contents

List of abbreviations

CJEU – Court of Justice of the European Union

CFR – Charter of Fundamental Rights of the European Union

DPA – Data Protection Act

DPD – Data Protection Directive

EU – European Union

GDPR – General Data Protection Regulation

LED – Law Enforcement Directive

p. (pp.) – Page(s)

PNR – Passenger Name Record

Introduction

We will dedicate our study into the comprehension of the data subject rights, regarding the processing of their personal data, under the scope of the main two important legal provisions of the European Union in this matter: the GDPR and the LED, particularly in the context of data sharing.

First, we believe that has the most importance for our purpose to generally compare the data subject rights under both the GDPR and the LED, since this will allow us to understand their differences relatively to the protection of the data subject.

Secondly, we will analyse and compare the automated processing of personal data, particularly the figure of profiling, and automated decisions understanding their differences and similarities in both regimes and the rights given to the data subject as well the legal obligations that falls into the controller.

Thirdly, we will focus on analysing the legal background that allows these personal data sharing, between the responsible party and third parties, take place. We will consider for our study the responsible party being a private company and the third-party being law enforcement authorities. Private companies, in order to pursue their purpose, collect their user's personal data, which translates in private companies having a high amount of personal data. For nowadays criminal investigations, this information collected by the private companies is of an extreme importance.

Furthermore, we will study concerning these data sharing: the associated principles of law; we will define the different applicable laws in the different stages of the processing of the personal data and scrutinize the different purposes of each scope.

To conclude, we will highlight the right of access and its practical application on the core of these data sharing, approaching both the GDPR and the LED.

1. The data subject rights scope of protection under the Directive and the GPDR –differences and why

The GDPR and the Law Enforcement Directive (LED) both came to force on May 2018 bringing with them a new change regarding data protection on the EU legal framework.

The material scope of the GDPR is positive defined on Article 2(1)[1] plus on Article 2(2) we found the scope where this regulation does not apply [2]. As for the material scope of the LED we can locate it on Article 2 of the LED. Furthermore, for the purpose of this studying is important to refer the Article 1 of the LED as it limits the purpose of this directive:

(...)lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

As we can observe on Recital 19 of the GDPR, that we will develop further in our present study, the GDPR itself also forwards the processing regarding the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties to the LED.

The GDPR and the LED are both defining the rules of processing personal data[3], within different purposes, and each of them sets a range of rights regarding the figure of the data subject.

---

[1] Article 2(1): "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

[2] Article 2(2) states: "This Regulation does not apply to the processing of personal data: (a)in the course of an activity which falls outside the scope of Union law; (b)by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c)by a natural person in the course of a purely personal or household activity; (d)by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.".

[3] Article 4 of the GDPR defines personal data as "(…) any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person 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;".

The Chapter III of the GDPR, between Article 12 and Article 23 inclusive, defines the rights of the data subject[4] regarding the processing of the individual's data, as on the LED the data subject rights can be found on Chapter III between Article 12 and Article 18, inclusive[5]. At this point we will analyse the general differences between both the GDPR and the LED on the subject's data rights as well to understand the reason of these differences. The points 2.1 and 2.2 will further focus on the analyses of specifics articles in both the GDPR and the LED.

The article 23 of the GDPR, alongside with the Recital 73, acknowledges the circumstances when the subject's right can be restricted, however the restriction of the rights are under the conditions set in this Article[6]. These rights can be restricted since they are not absolute rights[7] however, there are principles to be respected when the limitation of the right occurs. DOMINIQUE MOORE explains that behind this Article 23, we have to consider other EU provisions:

(...) Article 52 (1) of the Charter[8] accepts that limitations may be imposed on the exercise of the rights such as those set forth in Article 7 and 8 of the charter, as long as the limitations are provided by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality , are necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others.

The article 23(1) sets the conditions to that limitation/restriction: it has to respect the essence of the fundamental rights and freedoms; has to be a necessary and proportionate measure in a democratic society and has to safeguard the matters present between point (a) and (j) of this Article.

---

[4] The rights of the data subject present on Chapter III of the GDPR are the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object and the right not to be subject to a decision based solely on automated processing.

[5] The rights of the data subject present on Chapter III of the LED are the right to information, access, rectification, erasure or restriction of processing,

[6] DOMINIQUE MOORE explains that these conditions were inspired by the provisions on the Charter and in particular by Article 52. *Commentary on the EU general data protection regulation (GDPR). A commentary*, p.545

[7] As per DOMINIQUE MOORE "As the CJEU has underline, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.". Op.cit., p.545

[8] Charter of Fundamental Rights of the European Union.

Regarding the essence of the fundamental rights and freedoms CJEU has given in several occasions the opinion on this regarding privacy and data protection.[9]

The Article 23(1) also establishes the *how* this limitation should take form "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure".

Turning our perspective to the LED, we do not find a general article defining a set of rules to restrict the data subject rights as we've found in the GDPR. In the LED we have the right's restriction inside the norm that establishes the right[10] or we can also find a single article restricting a single right[11].

As we've now concluded our overall view of the data subject rights in both the GDPR and the LED, we will continue our study focusing in a form of automated processing, *profiling* and the automated decisions that occur fruit of this processing.

Personal data is intrinsically connected with profiling, as it will be used as the base to evaluate certain aspects related to a natural personal, and from that profile an automated decision will happen. This specific processing of personal data is extremely important either to a private company, or to law enforcement as it can, for example, establish a pattern.

In this context, as we will further explain, the right that has an essential importance to the data subject is the right of access.

---

[9] As per DOMINIQUE MOORE the CJEU opined that"(…) (1) mass data retention did not affect the essence of the right to privacy under article 7 CFR, since it did not lead to knowledge of the contact of electronic communications; (2) mass data retention did not affect the essence of the right to data protection under article 8 CFR, since certain principles of data protection and data security had to be respected by providers of electronic communications service or of public communications networks; (3) legislation permitting public authorities to have access to electronic communications on a generalized basis compromise the essence of article 7;(…)" Op. cit., p.553.

[10] Article 13(3) of the LED.

[11] As example, Article 15 of the LED "Limitations to the right of access".

1.1. Article 11 of the Directive and the Article 22 of the GDPR – Automated processing, including profiling, under both regimes, differences and similarities

Automated processing and profiling are increasing exponentially alongside the advances of new technologies both in public and private sectors.[12] This can be explained by a large percentage of the population holding a smartphone, a computer and for the proportional increase of internet connections that are done on a daily basis, which generates large amounts of data[13]. This data is collected for different reasons: data analyses allows companies to predict their users' behaviours or preferences; for commercial purposes and others.

PAUL DE HERT and HANS LAMMERANT define profile in a general way as "a set of characteristics, features and attributes with which a person or group can be discerned from another person our group"[14]". In particular, these authors refer to a specific form of profiling describing it as:

The form of profiling we have in mind is based on the use of Knowledge Discovery Databases (KDD, better known as data mining. The purpose of KDD is to find useful patterns in data, which can be gathered from different sources. The first stages of the process entail selecting and gathering data and preparing it for analyses. In the actual data mining data is analysed with the use of algorithms in order to discern patterns. (...) The final step consists in evaluating these patterns for their relevance. From these selected partners a profile can be derived.[15]

---

[12] As example: "Some of the sectors are banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making." Article 29 Data Protection Working Party (2018) *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, p. 5.

[13] NIŠEVIC, Maja – "Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR", *Global Privacy Law Review,* Issue 2, (2020), pp. 104-115, *https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/1.2/GPLR2020082*.

[14] LAMMERANT, H. and DE HERT, P. – "Predictive profiling and its legal limits: Effectiveness gone forever.", *Exploring the boundaries of big data*, Vol. 32, (2016), p. 145.

[15] Op. cit., p. 145.

Also, Article 4 (4) of the GDPR brings us the definition of profiling[16], while the Article 22 establishes the scope of protection[17] of the data subject when is subject to automated processing, including profiling and therefore, as a result, an automated decision can occur.

We believe it is pertinent to briefly point to the wording present on both articles regarding automated process, as we observe a slight difference. Article 4(4) of the GDPR refers to "any form of automated processing" as Article 22 of the GDPR refers to "solely on automated processing"[18]. Even though that profiling requires automated processing, a human involvement during the process does not remove the activity out of the definition[19].

As we move now to the scope of the LED, we can observe on Article 3(4) that profiling is defined using the exact wording as on the GDPR on Article 4(4). As starting to analyse in parallel the Article 11 of the LED with the Article 22 of the GDPR, we encounter a different wording as well what seems a different protection of the data subject right on this matter. The Article 11 of the LED on its number (1) sets a clear prohibition:

---

[16] Article 4(4) of the GDPR " 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".

[17] To this point is important to mention that regarding the need of protection of the individual's rights on such cases "(…) profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards.". Article 29 Data Protection Working Party (2017) *Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)*, adopted on 29 November 2017, p.11.

[18] Solely automated processing translates to no human involvement on the processing. However, the criteria for human involvement as given on by Article 29 Data Protection Working Party (2018) "To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision" means that has to be a significant involvement of the human factor, significant to the point to change de decision. Otherwise if insignificant human involvement in the automated processing was considered, the controller could fabricate this involvement in order to avoid the application of the Article 22 of the GDPR. See, Article 29 Data Protection Working Party (2018) *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, p. 21

[19] Article 29 Data Protection Working Party (2018) *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, p. 7.

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited (...).

As, on the contrary, the Article 22 (1) of the GDPR mentions a right as follows:

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Initially, this can give the impression that comparatively speaking the Article 11 sets a stronger protection, as it mentions a clear prohibition, as Article 22 sets it as a right that can lead to the interpretation that has to be invoked by the data subject to trigger the article application.[20]

Although the Article 22(1) of the GDPR states that "The data subject shall have the right (…)", the WP29, on the *2018 Guidelines*, advises that this article should be interpreted as a general prohibition and not as a right to be invoked by the data subject. The WP29 raises several rational and legal justifications to defend Article 22(1) as a prohibition: although Article 22 is under Chapter III of the GDPR[21], not all of the rights present on this chapter are rights that have to see an active exercise to be applied, Articles 13 and 14 are passive rights as are rights that fall under the obligation of the controller to fulfil and not on the data subject[22]; if the Article 22 was a right to be invoked by the data subject, then the article 22(2)(c) would be conflicting and inconsistent as it states "is based on the data subject's explicit consent", however is not possible for the data subject to both consent and object in the same processing.

LEE A. BYGRAVE also shares the opinion that the fact that Article 22 is placed on Chapter III, doesn´t necessarily define it as direct subject data right as Articles 13 and 14, both in Chapter III, cast this as a duty on the controller, not as a right to invoke by the data subject. Also, the author brings to the discussing the fact that this "prohibition-issue" should be analyse under the requirements that the GDPR states on fully automated decisional systems that involve systematic and extensive evaluation of data subjects". The

[20] On the analyse of LEE A. BYGRAVE "(…) Article 11 (1) LED is clearly expressed as a qualified prohibition (…)". Commentary on the EU general data protection regulation (GDPR). *A commentary*, p. 539.
[21] The Chapter III of the GDPR as mention above, states the data subject rights.
[22] Articles 15-18 and Articles 20-21 are rights where it falls into the data subject spectrum to active exercise its rights.

GDPR sets as a requirement that these systems have to be submitted to a "data protection impact assessment (DPIA) previously, and therefore the author concludes that this rule satisfies the control function of a qualified prohibition.[23]

Another difference found in the wording of both Article 11(1) of the LED and Article 22(1) of the GDPR is regarding the nature of the legal effects produced on the data subject. Article 11(1) states a prohibition only when "adverse legal effects"[24] or when there is a "significantly affect"[25] are produced as the Article 22(1) only mentions "legal effects" or "similarly significantly". Here we can acknowledge that the GDPR has a boarder scope of application than the LED.

In the GDPR, this prohibition can be overcome if one of the exceptions is verified. The Article 22 (2) of the GDPR enumerates three exceptions to this right as follows:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

For processing on the basis of the Article 22 (a) and (c) the GDPR establishes on Article 22 (3) that the controllers have to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.". Article 22 (2) (b) also establishes that the Union or Member state law that authorizes such process has to include "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests".

We can conclude that the data subject, both on Article 22 (1) and Article 22 (3) has therefore always a *right* to a human intervention, when concerning the reviewing of a

---

[23] Op. cit., p. 531.

[24] "A typical adverse effect resulting from automated decisions could be the application of increased security measures or surveillance by the competent authorities." Article 29 Data Protection Working Party (2017) *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017,* p.12.

[25] "(…) as for example in the case where a passenger is not allowed on board because registered in a black list, thereby expanding the scope of Article 11." Article 29 Data Protection Working Party (2017) *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017,* p.12.

fully automated decision, this right as the author LEE A. BYGRAVE states is exercised *ex post.*[26]

Article 11 of the LED do not establish any of the exceptions to the prohibition as article 22 (2) does, due to the purpose of processing under the scope of LED, *explicit consent of the data subject* or *contractual purposes* would not be possible under the LED as there is a "(…) clear imbalance of powers between the data subject and the controller(…)."[27]

Although the Article 11 of the LED has we have seen does not refer to any specific exception to this prohibition, on the last part of paragraph one, we find a exception based on either a law issued by the Member State where the controller is based, or authorized by the Union, that has to provide appropriate safeguards for the rights and freedoms of the data subject, as we've analyse in Article 22 (3), and additionally mentioning that at least there has to be the right to obtain human involvement on the controller part.

In Article 11 (1) of the LED we observe that is clearly missing the provision present on Article 22 that allows the data subject "to express his or her point of view and to contest the decision". The Recital 38 of the LED, however, mentions this provision:

(…)In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.(…)

We can conclude that, contrary to the GDPR, these *ex post* safeguards are not required under the LED, nevertheless, the Member States when transposing the directive to their national jurisdiction can provide to the data subject a higher level of protection as Recital 15 and Article 1 (3) states.[28]

Analysing now the special categories of personal data, defined in Article 10 of the LED, Article 11(2) of the LED only allows decisions, as the ones mention in paragraph 1, in the situation when the Member State has adopted "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place." The paragraph

---

[26] Op. cit., p. 538.
[27] Article 29 Data Protection Working Party (2017) *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017,* p.12.
[28] LYNSKEY, O. – "Criminal justice profiling and EU data protection law: Precarious protection from predictive policing." *International Journal of Law in Context*, 15(2), (2019), 162-176.

3 of the Article 11 is in accordance with the EU antidiscrimination law prohibiting profiling that will result in discrimination of individual's mention on Article 10.

Since this is extremely sensitive data, WP29, 2017 has reiterated the importance of the Member State to adopt rigorous safeguard measures when transposing the Directive, mentioning that when processing that specific data, there is the obvious existence of risks that can lead to discrimination.[29]

On the first part of Article 22(4) we encounter a qualified prohibition regarding automated decisions, as previously mention on Article 22(2), when that decisions are constructed upon processing of sensitive data as referred on Article 9(1). The author LEE A. BYGRAVE points that the prohibition mentions paragraph 2, instead of paragraph 1 of the Article 22, in order to highlight that the "prohibition takes precedence over the exception"[30].

Focusing now on the last part of Article 22(4), we can observe a derogation to this prohibition divided between the provisions present on Article 9(2)(a) and Article 9(2)(g), that allows the processing of this special categories data upon explicitly consent of the data subject, situation as we´ve already developed above is not possible under the LED, or in the case of substantial public interest, and in such case the domestic law:

has to be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[29] Op. cit., p.13.
[30] Op. cit., p.539.

1.2. Limitations of the right of access by the data subject under the Directive. Analysis of articles 14 ,15 and 16 of the Directive

The right of access is set as a general rule under Article 14 of the LED, the Member States therefore, must provide first to the data subjects the right to obtain the confirmation whether their data is being processed and access to the personal data that is being processed from the controller.[31] When this communication happens, Article 12(1) of the LED obliges the controller to provide this information "(…) in a concise, intelligible and easily accessible form, using clear and plain language.(…)".

Related to our present study, the Article 14(g) establishes that when the right of access is fully fulfilled, the controller has not only to communicate the personal data under processing but also the origin of this data. The WP29, 2017 advises that additionally, if possible, "(…) the purposes for which the data were transmitted (…)" should be part of this communication from the controller to the data subject.

The limitations to the right of access are set on Article 15 of the LED: these limitations can be fully or partially; the duration of these limitations are not clearly establish as they have to be adopted case by case, however the article defines that "(…)for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society(…). Once the exercise of the right of access no longer represents liability for the investigation in place, the right of access is restored again. The article 15 does not set any specific time frame for the restriction, however by the interpretation of the word of law, this restriction should not be definitive. The data subject that would receive this information, as the purpose is the *prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,* should be part of the criminal procedure and qualify as witnesses, victims, persons of interest, experts, convicts and suspects.

If no communication will take place from the controller to the data subject, and therefore the restriction on Article 15(1) applies, the concept of "neither confirm nor deny" can be applied, especially in the cases that the act to inform the data subject of the

[31] Article 29 Data Protection Working Party (2017) *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017,* p.19.

refusal or restriction undermine a purpose under paragraph 1, as per Article 15(3). This response leaves the data subject on a blank space and is expected that can result in frustration on the data subject side. On this case, the WP29, 2017 advises, in accordance with the last part of Article 15(3) , that the data subject has to be provided with information regarding the right to submit a complaint with the supervisory authority, the contact details of this DPA or presented with the option to pursue a judicial remedy. Here we can conclude that the Law Enforcement Authorities can either directly deal with the data subject request or indirectly, by Member States enforcing "(…) their supervision authorities to exercise data subject rights in case a controller decides to limit them."[32]

To complement this disposition, Article 15(4) states that Member States have to "(…) provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities."

The *right to rectification or erasure of personal data and restriction of processing* under Article 16, is an extremely important provision.

Analysing the rectification aspect, this importance is explained by the fact that if inexact data, especially when relating to facts[33], is being processed by the controller, adverse legal effects can occur for the data subject.

This said, a necessity raises to process, as urgent as possible, the founded requests to rectify data.[34]

The erasure of data is allowed by the article 16(2) when the processing of the data disobeys the LED as stated in Recital 47. The domestic legislation has to provide this right of erasure in the following situations as mention in the article: when it violates the principles of processing as in Article 4; when is unlawful, Article 8; when it violates the provision regarding special categories of personal data present in Article 10 and where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

---

[32] SAJFERT, Juraj and QUINTEL, Teresa – "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities" (December 1, 2017). *Cole/Boehm GDPR Commentary*, Edward Elgar Publishing, 2019, Forthcoming.

[33] As specified in Recital 47 of the LED.

[34] The WP29 advises that this requests with the purpose to rectify data should be done within a month. Article 29 Data Protection Working Party (2017) *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017,* p.21.

The WP29, 2017 points, the importance for the domestic legislators as well the controllers to do not interpretate the provisions enumerate on Article 16(2) as *exhaustive* and to do an interpretation of the article, alongside the core of the right defined in the Recital 47.[35]

There are however, two situations outlined by Article 16(3) when instead to erasure the data, the controller can restrict the processing of the data:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

We find pertinent to briefly mention the difference between the GDPR and the LED regarding the right to rectification and erasure. In the LED, as we have seen, these two rights are combined in one single provision, in Article 16. However, in the GDPR we find these rights allocated to different articles, as Article 17 is dedicated solely to the *right to erasure ('right to be forgotten')* and Article 18 sets the provision for the *right to restriction of processing.*

Overall, these rights represent a strong shield of protection to the data subject regarding the processing of his/her personal data. The legislator is aware of the impact of this information on the individual's core, especially since we are in the scope of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and established safeguards and mechanisms to be used even if the right is restricted, for example as we mention the possibility to submit a complaint with the supervisory authority when the right of access is restricted.

On the next point we will enter into the data sharing between a private company and a law enforcement authority. Since its personal data that will be the content of this transmission, we will understand how the data subject rights are affected, specially the right of access and which regime applies and regulates the different stages of the transmission.

[35] Op. cit., p. 21.

2. The data subject rights and data sharing between private companies and competent authorities

On a private company perspective, the data subject personal data that is collected[36] and therefore processed for commercial purposes falls under the material scope of the GDPR[37]. Focusing on a more "Silicon Valley" company perspective, high-tech companies such as Google, Facebook or Uber collect a huge amount of the user's data, not only but also, to be able to provide a personalize service to the user and to allow their platforms to maximize the user experience accordingly with the applicable privacy laws. These companies in order to collect the referred amount of data, have tools and resources that are not normally available to the common companies or even public institutions and organizations, such as Law Enforcement authorities.

Therefore, is not a surprise that Law Enforcement authorities all over the world would eventually understand the value of these companies and start to request data to them when pursuing a criminal investigation[38] when that data would be useful to identify the individual in question.

If we take a close look in the transparency reports of these high-tech companies[39] we can see an exponentially increase on this numbers, year by year. This shows us that official government authorities are using these platforms as tools to conduct their criminal investigations, they acknowledge their own limitations on this subject and make the smart move to take use of the high amount of data held by these companies creating this new reality between a private and a public figure inside the criminal investigation scene.

---

[36] The Article 4(2) of the GDPR defines processing as "(…) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.".

[37] In the words of HERKE KRANENBORG "The first paragraph of Article 2 positively formulates what is covered by the GDPR: the processing of personal data wholly or partly by automated means and other than by automated means when the personal data form part of a filling system are intended to form part of such a system. Article 2 does not differentiate between the public and private sectors", *Commentary on the EU general data protection regulation (GDPR). A commentary*, p.63.

[38] JASSERAND, Catherine – "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?", *Computer Law & Security Review* Volume 34, Issue 1, February 2018, pp. 154-155.

[39] Facebook has reported that between January 2019 and June 2019 more than 140,000 government requests for the disclosure of user's data based on a criminal request have been made, see *https://transparency.facebook.com/government-data-requests/jul-dec-2019*.

One of the questions that raised among us was which are the applicable laws when law enforcement authorities or competent authorities access data that initially was collected for a different purpose, a non-criminal purpose.

The GDPR excludes itself for the regulation of processing of personal data by competent authorities for prevention, investigation, detection or prosecution of criminal offences[40], in the other hand the LED on the Article 2 (2) enforces positively this regulation and shares with the GDPR, as per HERKE KRANENBORG, the same definition of "personal data", "processing" and "filling"[41]/[42]. We can so far establish that when the data is initially collected by a private company the initial purpose falls under the material scope of the GDPR and therefore the processing of that data will be regulated by the GDPR. When the data sharing happens, this transmission is still regulated by the GDPR.

After the data transmission, when the same data is being further processed by competent authorities[43] for the prevention, investigation, detection or prosecution of criminal offences, the purpose changes and it falls under the scope of the LED, at this stage that data is now subject to the rules of the LED. [44]

The recital 19 of the GDPR clearly forwards to the LED the regulation of the data when is being processed for the "(…) purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (…)". The same recital also establishes that a Member State can entrust a competent authority, as per the definition on the Article 3 (7) of the LED, with a duty that not falls under the above purpose for processing of personal data and that falls within the scope of the GDPR.

---

[40] Article 2(2)(d) of the GDPR.
[41] KUNER, C., BYGRAVE, L. A., & DOCKSEY, C. *Commentary on the EU general data protection regulation (GDPR). A commentary*. Kettering, Oxford University Press, (2019), p.7.
[42] The definition of "filing" can be found on Article 6 of the GDPR.
[43] LED has succeeded to define competent authorities on the Article 3 (7) as: "competent authority means: (a)any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b)any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".
[44] JASSERAND, Catherine – "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?", *Computer Law & Security Review* Volume 34, Issue 1, February 2018, p. 157.

The Recital 11 of the LED confirms the Recital 19 of the GDPR and forwards to the GDPR the cases where the Member state entrust a body or an entity – not a competent authority – to collect personal data and further processing for the purposes of investigation detection or prosecution of criminal offences in order to comply with a legal obligation.[45]

As we´ve seen, both the GDPR and the LED regulate this data however, in different stages of the processing. The GDPR in the initial moment when the data is being collected by a private company for a non-criminal purpose and the further processing of that data for the purposes of investigation detection or prosecution of criminal offences falls on the scope of the LED.

It´s also important to acknowledge and mention at this point a pertinent perspective on the legal background of the Article 2 of the GDPR.

On this HERKE KRANENBORG[46] compares the Article 3 of the DPD with the Article 2 of the GDPR concluding that they share in a large part the same positive formulation however in the exclusions, we can spot a big difference. That big difference is that the Article 2 of the GDPR mentions a specific set of rules regarding the law enforcement authorities and no longer broadly states, as the Article 3 of the DPD previously did, to "activities of the state in areas of criminal law". Also, as we mention before, the GDPR uniforms this exclusion of the LED scope not only with the Article 2 but also in the Recital 19. With this said, HERKE KRANENBORG states that there is more clarity now "(…) as to whether private entities are covered by the GDPR when they are providing information, they collected for commercial purposes to law enforcement authorities.".[47]

---

[45] The Recital 11 of the LED gives the example of the financial institutions : "(…) for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.".

[46] Op. cit., p.64.

[47] As an example, for the author, the PNR cases that were found outside the scope of the DPD by the CJEU, now would be considered to be covered by the GDPR, as the GDPR on the Article 2(2)(d) excludes itself only when the data is being processed by the competent authorities. In addition is pertinent to mention that the PNR cases have a specific regulation with the Directive (EU) 2016/681.

2.1. The new so-called Law Enforcement Response Teams

Now that we have understood the role of the GDPR and the LED on the process of data sharing, the other question that imposes itself is – how do this high-tech companies comply and response to this data requests?

As we can see on the transparency report done by Facebook, the data requests coming from competent authorities on a criminal basis are increasing exponentially year by year. Since this high-tech companies hold a great amount of data, not complying with these requests would not only depreciate the public image of these companies but also create tension between the national regulator of the respective service[48].

However, lawful principals as legality, proportionality, territoriality, necessity and complying with the applicable legal framework of each country have to be taken in account when complying with these legal data requests. This compliance demands a big change of operations for these companies.

EU based private companies such as Facebook, Uber, Booking, Twitter among many others, felt the necessity to create the conditions to comply to these requests and from that necessity resulted the creation of specialized teams known in general as Law Enforcement Response Teams.

To prevent a personal data breach[49] on these processes of data sharing, these companies created, as a first step, special interfaces[50] to ensure the legality and the legitimacy of the source of the requests. It is important to emphasize that these teams have the important mission to be the keepers of the "gate" regarding their user's privacy. Upon receipt of a data request from competent authorities there are a few principals to be

---

[48] On this matter is pertinent to mention that the car-sharing platform Uber, has a long dispute with the Transport for London to keep operating since their arrival to London. Since 2012 the car-sharing platform had to comply with different measures to keep their license. The most recent favorable decision, after the decision on November 2019, arrived this year with the approval of the license renewal. Two of the factors, among several, that contribute to this decision was the response to the data requests coming from the British Police and Metropolitan Police and the proactive reports that Uber continually does to Transport for London regarding on-platform safety incidents. As seen on different news websites such as: *https://www.dailymail.co.uk/news/article-8746659/Police-Ubers-licence-bid-taxi-firm-shares-data-intelligence-officers.html*; *https://www.thetimes.co.uk/article/uber-gives-police-private-data-on-drivers-and-passengers-dm7l3gsxv* and also accordingly to internal statements on *https://www.uber.com/en-GB/blog/how-uber-in-london-works-with-the-metropolitan-police/*.

[49] Article 4(12) of the. GDPR defines personal data breach as "'(…) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

[50] As example, the Uber law enforcement portal on *https://lert.uber.com/s/?language=en_US*; also Facebook as a similar portal that can be access on *https://www.facebook.com/records/login/*.

balanced on the equation between the data requested and the data shared, one of them is the proportionality principal. The proportionality principle, a universal and transversal principle to both national and EU legislation, present in national constitutional laws and EU treaties, is one of the most important principals of the EU[51]/[52]. As per the ECJ,[53] this principal is a general principle of law, the general qualification results that the proportionality principle can be applied to an indefinite number of law cases, distinguishing itself from a principle of law.[54] We can observe three basic criteria concerning the proportionality principle: *suitability, necessity and proportionality sensu stricto.* [55]

The suitability criteria, applying now this analysis to our present study, would be the relation between the data shared and the intended objective. As a first step, it is the essential to establish a relation between the data to be shared and acknowledge if that data will fulfill the intended objective, as in our study case, a criminal investigation. This is aligned with the provision present on Article 5(1)(c), as it states that the personal data as to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');". If the data is not adequate, relevant to fulfil the purpose of the processing, the suitability criteria will not be fulfilled.

The necessity criteria applied to our study, translates to understand if the data that has been requested is necessary for the purpose to conduct the criminal investigation in question. The final exercise is to acknowledge the nature of the crime on the bases of the data request *versus* the data that is being requested. On the proportionality *sensu stricto* we conduct a balance between the intrusion on the individual's personal data, and sub consequent damages that can result on her/her spectrum of rights, and the benefit of that data to the criminal investigation. We will give hypothetical examples concerning these criteria to comprehend how they are applied in the practical sense.

---

[51] This principle has been adopted in EU institutions such as the European Court of Human Rights and the European Court of Justice.
[52] The proportionality principle is present on the Treaty on European Union on Article 5(3) and (4).
[53] The ECJ has stated in many cases the proportionality principal as a general principal of law. See as an example case 265/87, Hermann SchraderHS Kraftfutter GmbH & Co. KG v Haupt- zollamt Gronau [1989] ECR 2237, 521.
[54] HARBO, T.-I. – "The Function of the Proportionality Principle in EU Law"*, European Law Journal*, 16, (2010), p. 165.
[55] MALISZEWSKA-NIENARTOWICZ, Justyna – "The Principle of Proportionality in the European Community Law- General Characteristic and Practical Application," *Pravni Vjesnik 24*, no. 1 (2008), p.91.

It would be extremely invasive in the user's data to share more than the minimum necessary data to identify the user in a crime for example of theft[56]. The minimum personal data[57] that can identify a user can be from name, telephone number, email address, identification number, to an IP registration number. In the other hand, there is data that is considered more invasive in the privacy spectrum of the user, due to its nature, such as biometric data[58] and GPS location and therefore demands another proportionality exercise when shared. As we´ve said, these teams are also the "gate" keepers of their company's user's privacy, they have the legal responsibility to balance the proportionality of data shared and data requested.

As a practical example: Law Enforcement is requesting data to a taxi car-sharing company on the basis of a criminal request where the purpose is the prevention of a crime inside the terrorism scope. Law enforcement requests GPS location of the trips of a user, that in this hypothetical scenario is signalized by Law Enforcement as a possible member of a terrorist organization, for the period of six months in order to assess his movements and identify possible addresses of interest with the goal to capture the subject. In this example the sharing of six months worthy of GPS data is proportional as law enforcement is trying to establish a pattern of the movements of the user for a specific time frame and also the serious suspicion, of the subject to be part of a terrorist organization represents a threat to the public safety. Also, the necessity element is in place as without that specific that law enforcement couldn´t establish the movements of the user in question, therefore the data is necessary to the investigation.

In other hypothetical example, if Law Enforcement requests to the taxi car-sharing company six months of GPS location regarding a user suspect of a simple theft that occurred on a specific day and location, in a first analyses it seems the data requested is not proportionable and in such case to protect a unjustified privacy invasion, these teams

---

[56] Example of the principle of prohibition of excess.
[57] Article 4(1) of the GDPR defines personal data in a broad way " 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person 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;(…)".
[58] Article 4(14) of the GDPR defines it as "(…) personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;" and Article 9 of the GDPR includes it on special categories of personal data.

may proactively narrow down the amount of information shared based on principals of proportionality and necessity.

Additionally, to this exercise of balancing the level of intrusion on the user's data privacy, other legal requirements have to be considered when sharing the data upon the receipt of a legal data request. As the GDPR is a regulation that has been adopted in the national legal framework by each EU Member State[59], national legal requirements have also to be taken in consideration when sharing the data: the national law of the country where the data controller is based[60]; the national law of each State Member to where the data is shared, or the national law of a third country.[61]

Alongside with these teams, that receive and reply to legal data requests, other internal stakeholders such as local legal counsels, privacy teams and police liaisons work together to ensure that this data sharing respects the applicable privacy laws.

One of the stakeholders that has a determinant role in the communication with law enforcement authorities and competent authorities is the Police liaison[62]. The Police liaison is an internal stakeholder that is the main bridge, communication wise, between the company and the competent authorities. His/her main functions vary between liaising with the competent authorities, alongside with the companies Public Policy teams, to build up strategies, partnerships, establish processes of response, protocols and even webinars to instruct to the competent authorities on the use of the proper portals and to enlighten them the different types of data that the company holds.[63]

The team structure and their internal processes are always evolving accordingly with the EU legal framework, public safety issues and also with the internal guidelines of the

---

[59] The GDPR has been in force on May 24, 2016 and it applies since May 25, 2018 as per Article 99 (1) and (2) of the GDPR.

[60] Uber BV is the data controller for the data of users on the European Economic Area, the United Kingdom and Switzerland and is has the Headquarters on the Netherlands; Facebook as their headquarters in Europe in Dublin, Ireland, being therefore the controller Facebook Ireland Ltd. The national law of the country where the controller has their Headquarters regulates the data.

[61] Even though our study will not focus on the data transfers of EU based companies with third countries or international organizations, it is important to briefly refer that on this matter the GDPR on Article 44 and Article 45 generally allows these data transfers to occur if there is an adequate level of protection in the respective third country or internal organization.

[62] Also commonly named as "Outreach".

[63]Crime Stoppers International in 2018 announced a partnership with Uber, see *https://csiworld.org/csi-news/crime-stoppers-international-and-uber-partnership-announced*. In a global view, Uber as available on their website de different types of partnerships to promote safety *https://www.uber.com/us/en/community/safety/* as also Twitter shares in their website a list of safety related partnerships, see https://about.twitter.com/en_us/safety/safety-partners.html.

company. One clear example of change regarding the workflow of the Law Enforcement Response Team specifically of Uber is that due to the current pandemic situation the Portal once dedicated only to legal data requests related to criminal offenses, has now an option to receive requests coming from the Public Health Departments.[64]

[64] Uber's portal name at the moment is "Uber Law Enforcement and Public Health Portal"

2.2.How does a company respect the Article 15 of the Directive when sharing third-party data with Law Enforcement Authorities?

As we've previously mention, upon a receipt of a request for personal data, law enforcement authorities usually disclose the position of the data subject in the criminal investigation. On this point we will disregard minor crimes such as simple theft, credit card fraud among others and we will focus on serious crimes that because of their nature can pose a serious threat to individuals and public security.

We will construct a hypothetical situation to serve as an example of the action on the company side: a taxi car-sharing company receives a data request regarding a homicide, law enforcement is requesting data regarding a subject that configures the figure of suspect, the company is able to identify the user and to share the requested information to law enforcement.

On this sharing of data, the company acknowledges a user that represents a threat to the other users of the platform. Allowing this user to continue to use the platform and therefore putting other users in risk would put the company in an accountable situation. Therefore, the company removes the user of the platform, but does not inform the user the reason that led to this removal as it could jeopardize the ongoing criminal investigation.

Giving the example of the United Kingdom, the legal document used to request personal data, as a section regarding the disclosure to the data subject where it states:

The subject of the request should not be given indication that this request has been made prior to consultation with the requesting officer. If (….) subsequently receives a request for a copy of this document under DPA for information, please contact the requesting officer prior to disclosure. Discloser of this request without authorization of the requester may constitute an offence under s82 of the Investigatory Powers Act 2016.

As we previously conclude, the data after shared is being process for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Therefore, if the company would inform the data subject of the request of law enforcement, upon the moment when the request is received, this could jeopardize the criminal investigation. Depending on the national law of each member

state, the company, after authorization from the law enforcement authorities, will disclose to the subject that a personal request has been made.

In these situations, the data subject observes his/her right of access clearly restricted, especially the right of access as stated on Article 15(1)(c) of the GDPR.

As we've previously concluded, the Article 23(1)(d) allows this restriction, consequently the data subject can see his/her right of access restricted in two sides: by the company, as will not communicate that the data has been requested complying with restriction of the GDPR and by the Law Enforcement authority, if this assesses to restrict the right of access, based on Article 15 of the LED.

When the right of access is restored, the company with authorization of the law enforcement authority can disclose the data request to the user and the data subject can access the information stated in Article 14 of the LED.

Conclusion

The material scope of the GDPR and the LED, as we've mention through our study, plays definitely a main role on the difference of the level of protection given to the data subject in both the regulation and the directive. On the LED side we observe that the data subject rights tend to shrink more than in the GDPR, justified with the purpose of the processing under the LED, however we were also able to see that the data subject is entitled ,when the restrictions occur, to safeguard measures and mechanisms to exercise his/her rights.

The main new subject we wanted to bring to analyse was the sharing of personal data between private companies and third parties, specifically with law enforcement authorities, settling that both laws in different stages of the processing apply to this data communication and also demonstrating how principles of Law are taking into consideration in a practical sense. Furthermore, we've showed that the right of access on the course of the data sharing can be restricted, not only in the LED side but also in the GDPR creating a simultaneous double restriction.

We believe we've demonstrated the importance of the regulation of the personal subject data, especially in a new era where personal data is more and more collected and flows constantly in the vast space that is the Internet.

Bibliography

CARUANA, M. – "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement", *International Review of Law,* Computers & Technology, 33, (2019), pp. 249-270.

MALISZEWSKA-NIENARTOWICZ, Justyna – "The Principle of Proportionality in the European Community Law- General Characteristic and Practical Application," *Pravni Vjesnik 24*, no. 1 (2008), pp.89-98

DE HERT, P. and PAPAKONSTANTINOU, V. – "The new police and criminal justice data protection directive: A first analysis." *New journal of European criminal law*, 7(1), (2016), pp. 7-19.

FERNÁNDEZ, Diego – "Where Is Online Privacy Going?", Global Privacy Law Review, Issue 1, (2020), pp. 55-60.

GIANCLAUDIO, Malgieri – "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations" *Computer Law & Security Review,* Volume 35, Issue 5,(2019).

HARBO, T.-I. – "The Function of the Proportionality Principle in EU Law". *European Law Journal,* 16, (2010) pp. 158-185.

JASSERAND, Catherine – "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?", *Computer Law & Security Review* Volume 34, Issue 1, February 2018, pp. 154-165.

KUNER, C., BYGRAVE, L. A., & DOCKSEY, 2C. "Commentary on the EU general data protection regulation (GDPR). A commentary." Kettering, Oxford University Press, (2019).

LAMMERANT, H. and DE HERT, P. – "Predictive profiling and its legal limits: Effectiveness gone forever.", *Exploring the boundaries of big data,* Vol. 32, (2016), pp. 145-173.

LEISER, Mark and CUSTERS, Bart – "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680," *European Data Protection Law Review (EDPL)* 5, no. 3 (2019), pp. 367-378.

LYNSKEY, O. – “Criminal justice profiling and EU data protection law: Precarious protection from predictive policing.” *International Journal of Law in Context, 15(2*), (2019), 162-176.

NIŠEVIC, Maja – “Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR”, *Global Privacy Law Review,* Issue 2, (2020), pp.104-115.

SAJFERT, Juraj and QUINTEL, Teresa – “Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities” (December 1, 2017). *Cole/Boehm GDPR Commentary*, Edward Elgar Publishing, (2019).