DATA PRIVACY AND DATA PROTECTION, DURING THE CURRENT COVID-19 PANDEMIC[1]

PRIVACIDADE E PROTEÇÃO DE DADOS, DURANTE A ATUAL PANDEMIA COVID-19

Manuel David Masseno[2]

Foreword: From the very beginning of the current Pandemic, the implementation of mobile applications designed for the location and tracking of infected persons appeared as one of the most promising answers in order to tackle the spread of Covid-19. As is well known, the EU - European Union has a remarkably robust Legal environment regarding Privacy and Data Protection. Therefore, the EU Institutions and competent bodies tried to address these issues in order to provide a common approach, or at least harmonized approaches, suitable to comply with the relevant rules. Being this a lecture and not an academic conference delivered to peers, we will start with an overview of the EU Legal framework concerning the processing of health-related personal data. Only after, will our focus turn to the pertinent statements from the Institutions and competent bodies.

1. The Legal Framework of Privacy and Data Protection at the European Union

Currently, is in place a microsystem based on the *General Data Protection Regulation*[3], also known as the *GDPR*. In addition, as our issue as to do with mobile

[1] Aula / Palestra proferida no dia 12 de junho de 2020 e destinada ao *LL.M. – Master of Laws* da *Unitedworld School of Law* da Universidade Karnavati, de Gandhinagar, Estado de Guzerate, na Índia, mas que foi seguida por várias centenas de Professores e Alunos de Pós-Graduação da Índia e do Paquistão, através da Internet. Sem pretensões no que se refere à Dogmática, este texto se assume enquanto tal, com a redução a escrito de um contributo oral destinado à formação de estudantes com conhecimentos limitados do Direito da Proteção de Dados da União Europeia.

[2] Professor Adjunto e Encarregado da Proteção de Dados do IPBeja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI- Mestrado em Engenharia de Segurança da Informação Pertence à EDEN Rede de Especialistas em Proteção de Dados da Europol Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, em Portugal; assim como, no Brasil, ao Grupo de Estudos de Direito Digital e *Compliance* da FIESP - Federação das Indústrias do Estado de São Paulo, à Comissão Estadual de Direito Digital da Ordem dos Advogados do Brasil, Seção de Santa Catarina e ainda à Comissão de Direito Digital da Subseção de Campinas da OAB.

[3] In full, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

devices, the *Directive on privacy and electronic communications*, or *ePrivacy Directive*[4], has an upmost role as the applicable *Lex specialis*.

Besides and after the *Treaty of Lisbon* (2007-2009)[5], Privacy and Data Protection have now a position at a Constitutional level, as fully recognised Fundamental Rights[6].

This, at the *TFEU – Treaty on the Functioning of the European Union*[7], as:

> 1. Everyone has the right to the protection of personal data concerning them.
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. (Article 16)

The same for the *Charter of Fundamental Rights of the of the European Union*[8], as

> Everyone has the right to respect for his or her private and family life, home and communications." (Article 7 – Respect for private and family life)

And, moreover,

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which

[4] As is generally known Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219>.

[5] The *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, signed at Lisbon, 13 December 2007 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT>.

[6] For a first and general approach to all these issues, FRA – European Union Agency for Fundamental Rights, together with the European Court of Human Rights / Council of Europe and the published the European Data Protection Supervisor published the *Handbook on European data protection law*, being available the 2018 edition, free of charge! <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf>.

[7] The *Treaty on the Functioning of the European Union*, formerly the *Treaty establishing the European Economic Community*, signed in Rome, the 25th March 1957 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT>.

[8] The *Charter of Fundamental Rights of the European Union*, solemnly proclaimed on 7 December 2000 by the European Parliament, the Council of Ministers and the European Commission as a *restatement* of the EU rules in place, has a full Legal, and Constitutional, status after the *Treaty of Lisbon* <https://eur-lex.europa.eu/eli/treaty/char_2012/oj>.

> has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority. (Article 8 – Protection of personal data)

Besides, the *Treaty of European Union*[9], the very *Constitutional core* of the EU, declares that

> The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities [...]. (Article 2).

Therefore,

> 2. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.
> 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law. (Article 6)

In addition, we need to take a due regard to the Case Law of the *two* European Courts.

For a first, the CJEU – Court of Justice of the European Union, as always, acted with a clear purpose, such as the consolidation of the EU Legal Order, including its standing vis-a-vis Member States Laws.

On our issue, Public or Private Electronic Surveillance, after assimilating the *Treaty of Lisbon*, the CJEU took data protection rights even more seriously than before,

[9] The *Treaty of the European Union*, originally signed at Maastricht, on 7 February 1992, and amended by the *Treaty of Amsterdam*, signed on 2 October 1997, and by the *Treaty of Nice*, signed on 26 February 2001 <https://eur-lex.europa.eu/eli/treaty/teu_2012/oj>.

namely by the Judgments on *Digital Rights Ireland*[10], *Google Spain*[11], *Schrems*[12], *Breyer*[13] and *Tele2 Sverige*[14] Cases.

On the other hand, is in place the ECHR – European Court of Human Rights, established on 21 January 1959, assuring the enforcement and implementation of the *European Convention on Human Rights*[15], of 1950, in the Member States of the Council of Europe[16], specifically:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Article 8 – Right to respect for private and family life)

The ECHR applied these Privacy provisions to its Judgements on Data Protection issues, notably in those connected to Surveillance and Health-related data[17], as in Peck

[10] Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland* Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Joined Cases C-293/12 and C-594/12 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293>.

[11] Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain* SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Case C-131/12 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>.

[12] Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian *Schrems* v Data Protection Commissioner. Case C-362/14 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>.

[13] Judgment of the Court (Second Chamber) of 19 October 2016. *Patrick Breyer* v Bundesrepublik Deutschland. Case C-582/14 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595847494490&uri=CELEX:62014CJ0582>

[14] Judgment of the Court (Grand Chamber) of 21 December 2016. *Tele2 Sverige* AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. Joined Cases C-203/15 and C-698/15 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595847793630&uri=CELEX:62015CJ0203>.

[15] In full, the *Convention for the Protection of Human Rights and Fundamental Freedoms*, open for signature in Rome, the 4th November 1950 <https://www.echr.coe.int/pages/home.aspx?p=basictexts>

[16] The Council of Europe, founded by the *Treaty of London*, signed at the 5th May 1949, is a regional international organization that aims to promote Human Rights, Democracy and the Rule of Law, without organic connections with the European Union.

[17] Clearly, the ECHR had in mind the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* – Convention 108, also of the Council of Europe, signed on the 28 January 1981, the first and paramount international reference as for Personal Data Protection <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

v. The United Kingdom, of 2003[18], in I v. Finland, of 2008[19], in S. and Marper v. the United Kingdom, also of 2008[20], and in Zakharov v. The Russian Federation, of 2015[21].

2. The relevant Processing of Personal Data

As for the *GDPR*, very broadly, "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 (Article 4 1).

With particular rules for "sensitive data", including

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation […] (Article 9 (1) - Processing of special categories of personal data).

Namely, "data concerning health", that, in this context,

> means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; (Article 4 (15)

Thus, the "Processing" of personal data, in general, notwithstanding "data concerning health",

> 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,

[18] Judgment in the case of *Peck v. the United Kingdom* (application no. 44647/98), of 28 January 2003 <http://hudoc.echr.coe.int/eng?i=001-60898>.
[19] Judgment in the case of *I v. Finland* (application no. 20511/03), of 17 July 2008 <http://hudoc.echr.coe.int/eng?i=001-87510>.
[20] Judgment in the cases of *S. and Marper v. the United Kingdom* (applications no. 30562/04 and 30566/04), of 4 December 2008 <http://hudoc.echr.coe.int/fre?i=001-90051>.
[21] Judgment in the case of Roman *Zakharov v. The Russian Federation* (application no. 47143/06), of 4 December 2015 <http://hudoc.echr.coe.int/fre?i=001-159324>.

> use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (Article 4 (2)

And, in any case,

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; […] (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; [or] (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; […] (Article 6 (1) – Lawfulness of processing)

However,

> […] It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health […] (Recital 45)

Having in mind that,

> Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread […] (Recital 46)

As well as the

> Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. […] (Recital 52)

Accordingly,

> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. (Article 24 (1) – Responsibility of the controller)[22]

Therefore,

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. [besides]
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. (Article 25 – Data protection by design and by default)[23]

Hence,

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of

[22] As, "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;" (Article 4).

[23] On these, are in place *the Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default*, adopted by the European Data Protection Board, on 13 November 2019 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>.

> security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; […] (Article 32 – Security of processing)

and,

> 1.Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. […]
>
> 2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9 (1) […]; or (c) a systematic monitoring of a publicly accessible area on a large scale. (Article 35 – Data protection impact assessment)[24]

Consequently, when "Processing of special categories of personal data", such as "health related data", the generic prohibition of such processing "shall not apply [if]

> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes [or]; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

So

> Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. (Article 9 (1) (2)

[24] On this issue, the Article 29 Working Party adopted the *Guidelines on Data Protection Impact Assessment (DPIA)* (wp248rev.01), on 4 April 2017, last revised and adopted on 4 October 2017 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

In short,

> Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes[…] (Recital 53)

Besides,

> Decisions […] shall not be based on special categories of personal data referred to in Article 9(1) […] (Article 22 (4) – Automated individual decision-making, including profiling)[25]

Summarising, "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')". Thus, observing the Principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', respecting 'integrity and confidentiality' of such data (Article 5 – Principles relating to processing of personal data).

Also for the purpose of facing an exceptional Public Health[26] menace, such as this Pandemic, the *GDPR* has explicit provisions on the "Restriction of rights".

Following, both, the *Charter of Fundamental Rights of the European Union* (Article 52 (1) – Scope and interpretation of rights and principles), and the *European Convention*

[25] As, "'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;" (Article 4 (4). Regarding these issues, the Article 29 Working Party adopted the *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01), of 3 October 2017, last revised and adopted on 6 February 2018 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

[26] Therefore, "[…] 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [of 16 December 2008 on Community statistics on public health and health and safety at work] namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality […]." (Recital 54)

of Human Rights (Article 8 (2) – Right to respect for private and family life), these assert that

> 1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including […] public health […];
> 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction. (Article 23 (1) – Restrictions)

3 – The Institutional Pronouncements

After the previous outline of the rules in plane, the assessment of the Pronouncements becomes a much easier endeavour.

The earliest was the *Statement on the processing of personal data in the context of the COVID-19 outbreak*, adopted on 19 March 2020, by EDPB – the European Data Protection Board[27]-[28].

[27] Available here <https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_en>.

[28] Regulated from Article 68 to Article 76, as at Recital 139, "In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of

For a first, the EDPB made clear that the *GDPR* does not prevent public health authorities and employers from processing personal data in order to fight against the current Pandemic, namely health related data and location data.

Besides, regarding employment contexts, is said that employers should follow national workplace health and safety regulations, as well as public health rules, as in Art. 9 (1) (i), also for the vital interests of their employees or other persons, as in Art. 9 (1) (c), as those in Art. 9 (1) (h) were not designed addressing for such emergencies.

Then, for the processing of electronic communications data, in special for location, underlines that *ePrivacy Directive*, as in Art. 15(1), allows national implementing laws to restrict the scope of the provided rights "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security", with an emphasis on anonymization minimization, in addition to strict proportionality requirements.

Moreover, present and future National laws and regulations are under judicial review by, both, the Court of Justice of the European Union and the European Court of Human Rights, following the criteria at the *European Charter of Fundamental Rights* and at the *European Convention of Human Rights*, as stated by the CJEU at *Tele2 Sverige*.

Summarizing, the EU Data Protection Laws are to be applied, respecting its core Principles and the rights of the data subjects, as much as possible.

About a month later, the EDPB issued its *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, adopted on 21 April 2020[29].

Based on Art. 70 (1) (e) of *GDPR* and to be enforced by each national supervisory authority, these *Guidelines* enhance and specify the contents of the previous *Statement*, enhancing the role of the *GDPR* and the *ePrivacy Directive* as the utmost references, also for Member States.

About the use of location data, both from electronic communications operators and information society services providers, the consent of the user would always be

the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.".

[29] Available here <https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en>.

needed[30], unless a National law introduced a derogation following the said requirements, with an emphasis on anonymized data, even being aware of its technical shortcomings[31].

For contract tracing, the EDPB pointed out the scope and functions of Principles, such as purpose limitation and minimization, together with privacy by design and privacy by default requirements.

In addition, other Principles as those of "lawfulness, fairness and transparency, together with "purpose limitation" and "storage limitation", including the so called "sunset clauses", should be present, with all data erased when no longer strictly necessary. The same for "integrity and confidentiality", with the identification of mobile devices being pseudonymized and the retained data encrypted.

Equally, the transparency of all procedures has to be assured, including the auditability of algorithms by independent experts.

For its part and also in early April, the Commission, the Executive branch of the European Union, approved the *Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data* of 8 April 2020[32]-[33].

The Commission advocates for a common, "pan-European", approach, foreseeing the build-up of a toolbox of practical measures, with the participation of Member States, together with EU Institutions and Agencies[34], while drafting a least intrusive legal framework for mobile applications.

About a week later, the Communication from Commission *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*[35], came out.

---

[30] As, " 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;" (Article 4 (11)

[31] On these, the Article 29 Working Party had adopted *Opinion 05/2014 on "Anonymisation Techniques* (WP216), on 10 April 2014 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

[32] C(2020)2296final, of 8 April 2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518>.

[33] According to Article 288 of *TFEU*, recommendations "have no binding force", but may have an important political role as a minimum consensus was reached.

[34] Such as the European Centre for Disease Control, the Health Security Committee, the Body of European Regulators for Electronic Communications, the Networks and Information Security Cooperation Group, ENISA – the European Cybersecurity Agency, Europol – the European Police Agency, along with EDPB and the European Data Protection Supervisor.

[35] 2020/C 124 I/01, of 17 April 2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29 >.

Communications are not binding, but performing the role of "Guardian of the Treaties", the Commission overseas the implementation of EU Law. Moreover, as the foreseen common approach didn't happen… the Commission restated the requirements of National acts in order to comply with EU Law.

REFERÊNCIAS

COE – Council of Europe [CE – Conselho da Europa]. Convention for the Protection of Human Rights and Fundamental Freedoms, open for signature in Rome, the 4th November 1950 [Convenção Europeia dos Direitos Humanos / Direitos do Homem] <https://www.echr.coe.int/pages/home.aspx?p=basictexts>.

_____. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Convention 108, also of the Council of Europe, signed on the 28 January 1981 [Convenção Europeia sobre a Proteção de Dados] <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

CJEU – Court of Justice of the European Union [Tribunal de Justiça da União Europeia]. Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland* Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Joined Cases C-293/12 and C-594/12 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293>.

_____. Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain* SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Case C-131/12 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>.

_____. Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian *Schrems* v Data Protection Commissioner. Case C-362/14 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>.

_____. Judgment of the Court (Second Chamber) of 19 October 2016. *Patrick Breyer* v Bundesrepublik Deutschland. Case C-582/14 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595847494490&uri=CELEX:62014CJ0582>

_____. Judgment of the Court (Grand Chamber) of 21 December 2016. *Tele2 Sverige* AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. Joined Cases C-203/15 and C-698/15 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595847793630&uri=CELEX:62015CJ0203>.

[European] Commission [Comissão Europeia]. Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis (C(2020)2296final), of 8 April 2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518>.

_____. Communication Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01), of 17 April 2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29>.

ECHR – European Court of Human Rights [Tribunal Europeu dos Direitos do Homem / Corte Europeia dos Direitos Humanos]. Judgment in the Case of Peck v. the United Kingdom (application no. 44647/98), of 28 January 2003 <http://hudoc.echr.coe.int/eng?i=001-60898>.

_____. Judgment in the Case of I v. Finland (application no. 20511/03), of 17 July 2008 <http://hudoc.echr.coe.int/eng?i=001-87510>.

_____. Judgment in the Cases of S. and Marper v. the United Kingdom (applications no. 30562/04 and 30566/04), of 4 December 2008 <http://hudoc.echr.coe.int/fre?i=001-90051>.

_____. Judgment in the case of Roman Zakharov v. The Russian Federation (application no. 47143/06), of 4 December 2015 <http://hudoc.echr.coe.int/fre?i=001-159324>.

EDPB – European Data Protection Board [CEPD – Comité Europeu para a Proteção de Dados, previously Article 29 Working Party / Grupo de Trabalho do Art.° 29.°]. Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

_____. Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), on 4 April 2017, last revised and adopted on 4 October 2017 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

_____. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), of 3 October 2017, last revised and adopted on 6 February 2018 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

_____. Guidelines on Article 25 - Data Protection by Design and by Default, no. 4/2019, adopted on 13 November 2019 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>.

_____. Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020 <https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_en>.

_____. Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, no. 04/2020, adopted on 21 April 2020 <https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en>.

EU – European Union [UE - União Europeia]. Charter of Fundamental Rights of the of the European Union, proclaimed on 7 December 2000, with the wording adopted on 26 November 2012 [Carta dos Direitos Fundamentais da União Europeia] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>

_____. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219>.

_____. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27/04/2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Regulamento Geral sobre a Proteção de Dados] <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

_____. Treaty establishing the European Economic Community, signed in Rome, the 25th March 1957 [Tratado instituindo a Comunidade Económica Europeia / Tratado de Roma] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT>.

_____. Treaty of the European Union, originally signed at Maastricht, on 7 February 1992, and amended by the Treaty of Amsterdam, signed on 2 October 1997, and by the Treaty of Nice, signed on 26 February 2001 <https://eur-lex.europa.eu/eli/treaty/teu_2012/oj>.

_____. Treaty amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, the 13th December 2007 [Tratado de Lisboa] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT>.

FRA – European Union Agency for Fundamental Rights [Agência da União Europeia para os Direitos Humanos] / ECHR – European Court of Human Rights / Council of Europe / EPDS – European Data Protection Supervisor [Autoridade Europeia para a Proteção de Dados]. Handbook on European data protection law, 2018 edition [Manual oficioso de várias Instituições, tanto da União Europeia quanto do Conselho da Europa] <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf>.