Rights, Equality and Citizenship (REC)

Programme of the EU Commission

(2014-2020)

Monitoring and Detecting Online Hate Speech

D2.2

Identification and analysis of the legal and ethical framework

Abstract: The current study sheds light on the content and on the scope of protection of the right to privacy, the right to personal data protection, the right to freedom of expression, the right to presumption of innocence, the right to non-discrimination, the right to freedom of assembly, the right to freedom of movement, the right to liberty and security, and the freedom to conduct a business, in the extent they might concern the MANDOLA research and outcomes. Its purpose is to feed the tasks that aim to ensure the legal and ethical compliance of the MANDOLA research (2.3), to assess the potential impacts of MANDOLA outcomes on rights and freedoms (2.4), and to discuss the potential impacts on these rights and freedoms of the definition of illegal online hate speech (2.1).

Contractual Date of Delivery	30 September 2016
Actual Date of Delivery	12 July 2017
Deliverable Security Class	Public
Editor	Estelle De Marco
Contributors	Experts mentioned in Section 7
Quality and Ethical Assurance	Tatiana Synodiou

The *MANDOLA* consortium consists of:

FORTH	Coordinator	Greece
ACONITE	Principal Contractor	Ireland
ICITA	Principal Contractor	Bulgaria
INTHEMIS	Principal Contractor	France
UAM	Principal Contractor	Spain
UCY	Principal Contractor	Cyprus
UMO	Principal Contractor	France

Document Revisions & Quality Assurance

Internal Reviewer:

Tatiana Synodiou, Associate Professor, Law Department University of Cyprus, Chair of the Ethics Committee of Mandola.

Revisions

Version	Date	By	Overview
v.2.2.0	08/06/2017	Inthemis (FR) Estelle De Marco as editor	First full version of the study.
v.2.2.1	19/06/2017	Inthemis (FR) Estelle De Marco as editor	Second version taking into account comments from contributing experts for Greece, Germany and Spain.
v.2.2.2	28/06/2017	Inthemis (FR) Estelle De Marco as editor	Third version taking into account comments from contributing experts for Bulgaria, Ireland, Netherlands and Romania
v.2.2.3	04/07/2017	Inthemis (FR) Estelle De Marco as editor	Fourth version taking into account comments from contributing experts for Belgium and Cyprus.
v.2.2.4	12/07/2017	Inthemis (FR) Estelle De Marco as editor	Slight modifications and clarifications taking into account new comments from the Bulgarian expert and Tatiana Synodiou's comments as quality assurance reviewer.

Table of Contents

1 Executive summary

The MANDOLA research and the MANDOLA outcomes may limit or threat some fundamental rights and freedoms, including the right to privacy, the right to personal data protection, the right to freedom of expression, the right to presumption of innocence, the right to non-discrimination, the right to freedom of assembly, the right to freedom of movement, the right to liberty and security, and the freedom to conduct a business. In this context, tasks 2.3 and 2.4 of the MANDOLA research aim to ensure the legal and ethical compliance of this research and to assess the actual impacts on these rights and freedoms of the MANDOLA outcomes. Task 2.1 of the MANDOLA research also discusses the potential impacts on these rights and freedoms of the definition of illegal online hate speech.

The current study is a precondition to these tasks, aiming at shedding light on the content and on the scope of protection of the above-mentioned rights and freedom in the extent they might concern the MANDOLA research and outcomes.

2 Introduction

2.1 Background to the MANDOLA project

MANDOLA (Monitoring ANd Detecting OnLine hAte speech) is a 24-months project co-funded by the Rights, Equality and Citizenship (REC) Programme of the European Commission, which aims at making a bold step towards improving the understanding of the prevalence and spread of online hate speech and towards empowering ordinary citizens to report hate speech.

2.1.1 MANDOLA objectives

The MANDOLA specific objectives are the following:

- to monitor the spread and penetration of online hate-related speech in the European Union (EU) and in the EU Member States using big-data approaches, while investigating the possibility to distinguish, among monitored contents, between potentially illegal hate-related speech and non-illegal hate-related speech;
- to provide policy makers with actionable information that can be used to promote policies for mitigating the spread of online hate speech;
- to provide ordinary citizens with useful tools that can help them deal with online hate speech irrespective of whether they are bystanders or victims;
- to transfer best practices among EU Member States;
- to set-up a reporting infrastructure that will enable the reporting of potentially illegal hate speech.

The MANDOLA project addresses the two major difficulties in dealing with online hate speech: the lack of reliable data and the poor awareness on how to deal with the issue. Indeed, it is difficult to find reliable data that can show detailed online hate speech trends (inter alia in terms of geolocation and in relation to the focus of hate speech). Moreover, available data generally do not distinguish between potentially illegal hate speech and not illegal hate speech. In addition, the different legal systems in various Member States make it difficult for ordinary people to perceive the boundaries between both these categories of content. In this context, citizens might have difficulties to know how to deal with potentially illegal hate speech and how to behave when facing harmful but not illegal hate content. The lack of reliable data also prevents to make reliable decisions and push policies to the appropriate level.

The two MANDOLA innovations are (1) the extensive use of IT and big data to study and report online hate, and (2) the research on the possibility to make a clear distinction between legal and potentially illegal content taking into account the variations between EU Member States legislations.

MANDOLA is serving: (1) policy makers - who will have up-to-date online hate speech-related information that can be used to create enlightened policy in the field; (2) ordinary citizens - who will have a better understanding of what online hate speech is and how it evolves, and who will be provided with information for recognising legal and potentially

illegal online hate-speech and for acting in this regard; and (3) witnesses of online hate speech incidents - who will have the possibility to report hate speech anonymously.

2.1.2 MANDOLA Activities

In order to achieve the set up objectives the project envisages the following activities:

- An analysis of the legislation on illegal hate-speech at the European and international level and in ten EU Member States.
- An analysis of the applicable legal and ethical framework relating to the protection of privacy, personal data and other fundamental rights in order to implement adequate safeguards during research and in the system to be developed. This analysis is the subject of the current report.
- The development of a monitoring dashboard, which aims to identify and visualise cases of online hate-related speech spread on social media (such as Twitter) and on the Web.
- The creation of a multi-lingual corpus of hate-related speech based on the collected data. It will be used to define queries in order to identify Web pages that may contain hate-related speech and to filter the tweets during the pre-processing phase. The vocabulary will be developed with the support of social scientists and enhanced by the Hatebase (http://www.hatebase.org/).
- The development of a reporting portal. It will allow Internet users to report potentially illegal hate-related speech material and criminal activities they have noticed on the Internet.
- The development of a smart-phone application. It will allow anonymous reporting of potentially hate-related speech materials noticed on the Web and in social media.
- The creation and dissemination of a Frequently Asked Questions document. It will be disseminated via the project portal and the smart-phone app.
- The creation of a network of National Liaison Officers (NLOs) of the participating Member States. They will act as contact persons for their country and will exchange best practices and information. They will also support the project and its activities with legal and technical expertise when needed.
- The development of a landscape of current responses to hate speech across Europe and of a Best Practices Guide for responding to online hate speech for Internet industry in Europe.

2.2 Purpose and scope of the study

The purpose of the current report is to present the outcomes of the analysis of the applicable legal and ethical framework relating to privacy, to personal data and to other fundamental rights protection in order to feed other tasks and enable, during the performance of these latter, the consideration of these rights where the project and its outcomes may have negative impacts on them.

Therefore, this task aims at identifying and analysing the above-mentioned framework to the extent that it may concern the MANDOLA research and the MANDOLA outcomes aiming at contributing to the fight against online hate-related speech.

Several rights that might be impacted, in addition to the right to privacy and to personal data protection, have been identified. They are namely the right to freedom of expression, the

right to presumption of innocence, the right to non-discrimination, the right to freedom of assembly, the right to freedom of movement, the right to liberty and security, and the freedom to conduct a business. The study focuses mainly on the legal instruments that protect these rights, on the definition of these rights and on the extent of their protection, without addressing the incrimination of threats to personality and of acts of discrimination and hate which will be the focus of the MANDOLA deliverable D2.1, together with issues of liability. This study moreover investigates more deeply some rights that appear more likely to be impacted by the project, namely the right to privacy, the right to personal data protection, and the right to freedom of expression, and the other rights in less detail, considering the need to confine the study to a reasonable number of pages.

The current study focusses on the European law, including the EU's Charter of Fundamental Rights, and on the European Convention on Human Rights, which are both binding for EU Member States, taking into account MANDOLA partners' potential national specificities where valuable. At the EU level, all the current data protection instruments are taken into account, in addition to the new Regulation and Directive that respectively replace the Directive 95/46/EC and the Council Framework Decision 2008/977/JHA.

2.3 Document structure

The document is structured as follows.

Section 1 provides an executive summary.

Section 2 provides an introduction.

Section 3 identifies the legal and ethical framework to be studied.

Section 4 analyses the legal bases and scopes of the fundamental rights at stake.

Section 5 provides a conclusion.

Section 6 provides the list of the experts who have contributed to the current study.

3 Identification of the legal and ethical framework

3.1 The need for identifying the legal and ethical framework

As already exposed, the aim of the MANDOLA project is to contribute to the combat against online hate speech, through (1) the analysis of the legal prohibitions of hate speech in ten EU Member States, and the formulation of recommendations in this regard, through (2) the creation of information to be provided to Internet users (awareness) and other stakeholders (best practices and recommendations), through (3) the creation of a dashboard that will enable to monitor impersonally the spread of hate speech, and through (4) to the development of mechanisms that will enable Internet users to report online hate speech.

Even though the combat against hate speech appears to the MANDOLA consortium as being crucial, all the measures taken in this purpose, and primarily those envisioned by the MANDOLA consortium, are susceptible to limit other human rights than the right to dignity and to non-being discriminated against.

In this context, two fundamental questions need to be discussed.

The first question is whether current measures that are taken against hate speech, which pursue the objectives of prohibition, prevention and repression, are the most appropriate in terms of opportunity. For example, a debate do exist between voices that call for strong proactive actions aiming at preventing hate-speech (or more generally illegal content) through a systematic censorship (and therefore a removal from servers and/or an ISP blocking)[1], and other experts who raise, on the opposite, that crimes should be punished and not hidden[2], and that combatting hatred rather demands education and adapted public policies[3]. The MANDOLA partners are not entitled to settle such a debate (which might reflect two different societal choices[4]), but to expose all the existing arguments and to identify best practices that appear to constitute a fair equilibrium between the combat against hate and the protection of other human rights, as objectively as possible, in order to further feed this interesting discussion that should take place before Parliaments. This exercise is proposed in the MANDOLA deliverables D2.1, D4.1 and D4.2.

The second question is whether the four actions, referenced above and proposed by the MANDOLA consortium, do respect other fundamental rights at stake. This question will be answered in the MANDOLA deliverable D2.3 as regards the MANDOLA research and in

[1] See Wikipedia, Internet censorship, https://en.wikipedia.org/wiki/Internet_censorship; Robert D. Atkinson, The Internet Is not (Fully) Open, nor Should It Be, 13 August 2015, http://www.innovationfiles.org/the-internet-is-not-fully-open-nor-should-it-be/ (last accessed on 24 November 2016).

[2] See European Digital Rights, "Internet blocking - crimes should be punished and not hidden", https://edri.org/wp-content/uploads/2013/12/blocking_booklet.pdf (last accessed on 24 November 2016).

[3] See for example Iginio Gagliardone, Danit Gal, Thiago Alves, Gabriela Martinez, Countering online hate speech, UNESCO, 2015, especially pp. 46 and s., http://unesdoc.unesco.org/images/0023/002332/233231e.pdf (last accessed on 24 November 2016).

[4] The question of whether each antagonist measure is necessary and proportionate in a democratic country being sometimes interpreted differently according to the country, as we will analyse it further in this report.

Deliverable D2.4 as regards the outcomes of the MANDOLA project. To serve as a basis of these deliverables, the current report must identify the other fundamental rights at stake, and identify their content and the extent of their legal protection.

3.2 Legal instruments that serve as a basis for the current study

Most of fundamental rights are protected by several instruments at International, European and domestic levels. In the course of the current study, main ones will be mentioned, but we have chosen to mainly base our analysis on the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Right (ECHR), and, to the extent necessary, on the EU Charter of Fundamental rights (EUCFR), which has the same value as the treaties since the entry into force of the Treaty of Lisbon[5], and which has the same meaning and scope as the ECHR, even though European Union law may provide more extensive protection[6]. The European Court of Justice, which is competent to judge on the violations of the EUCFR, makes its decisions in consideration of both the EUCFR's and the ECHR's requirements. Finally, it ought to be noted that the EU is in the process of accession to the ECHR[7].

This choice is primarily based on the fact that the ECHR is binding for States Parties, which number is of 47[8], including all the EU Member States[9]. These latter must firstly abstain from any arbitrary interference with protected rights, and have secondly the positive obligation "*to secure the rights and freedoms of persons within* (their) (...) *jurisdiction*"[10], which means that they have the positive obligation to ensure the respect of these rights "*even in the sphere of the relations of individuals between themselves*"[11], principle to which legal experts refer by using the formula "*Convention's horizontal effect*"[12]. In addition, the European Court

[5] Article 6 of the Treaty on European Union.

[6] EU Charter of Fundamental Rights, article 52, 3. For further reading, see especially French Cour de cassation, "Dossier : la charte des droits fondamentaux - historique et enjeux juridiques", *in* veille bimestrielle de droit européen, October 2010, n° 34, http://www.courdecassation.fr/publications_26/publications_observatoire_droit_europeen_2185/veilles_bimestrielles_droit_europeen_3556/2010_3865/octobre_2010_3810/droits_fondamentaux_18630.html (last accessed on 24 May 2017).

[7] Council of Europe, Accession of the European Union, http://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c= (last accessed on 24 May 2017).

[8] Council of Europe, Who we are, http://www.coe.int/en/web/about-us/who-we-are (last accessed on 24 May 2017).

[9] Since they have all accessed to or ratified the ECHR.

[10] On the basis of Article 1 of the ECHR. See ECTHR gr. ch., 17 February 2007, *Gorzelik and others v. Poland*, appl. n°44158/98, § 94, http://hudoc.echr.coe.int/eng?i=001-61637 (last accessed on 31 May 2017).

[11] ECtHR, ch., 26 March 1985, *case X. and Y v. The Netherlands*, appl. n° 8978/80, §23, http://hudoc.echr.coe.int/eng?i=001-57603; ECtHR, 3rd Sect., 24 June 2004, *von Hannover v. Germany*, appl. n°59350/00, §57, http://hudoc.echr.coe.int/eng?i=001-61853 (URLs last accessed on 12 May 2017).

[12] See for example Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 9, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984; ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity*, Council of Europe/European Court of Human Rights, December 2011, p. 4,

of Human Rights (ECtHR) had ruled 10,000 decisions in September 2008[13], which enables a deeper and very practical understanding of the ECHR provisions.

How the European Convention on Human Rights is transposed into legal local systems varies from country to country. Generally, the obligation to achieve the result of respecting treaties related to Human Rights by states[14], which cannot require the principle of reciprocity[15], is executed through law, but countries stay free to use the means they deem appropriate to reach that aim[16], in accordance with their Constitution[17]. As a result, the place of the Convention into the norms hierarchy is not the same in each country that respects the international text.

For instance, the Convention has been directly integrated into the local legal system by the Constitution in the Netherlands, Belgium, Spain and Bulgaria, and has been integrated by a law in Malta, Finland, Denmark, Iceland, Norway, United Kingdom and Sweden. As regards the place of the Convention into the norms hierarchy, it has a supra-constitutional force in the Netherlands, a constitutional force in Austria, an infra-constitutional but supra-legal force in Belgium, Greece, Swiss and Spain, and a simple legal force in Germany, Turkey and Finland[18]. In France, the Convention is directly integrated into the local system by the Constitution, as its article 55 states that "*Treaties or agreements duly ratified or approved shall, upon publication, prevail over Acts of Parliament, subject, with respect to each*

---

http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf (URLs last accessed on 30 May 2017).

[13] European Court of Human Rights, The Court in brief, accessible from http://www.echr.coe.int/Pages/home.aspx?p=court&c= at http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (last accessed on 12 May 2017).

[14] See Claudia Sciotti-Lam, *L'applicabilité des traits internationaux relatifs aux droits de l'homme en droit interne*, thesis, Bruylant Bruxelles, 2004, p. 35 *et seq*.

[15] See Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 and seq., especially p. 28: "*The Convention has from its earliest days been regarded as articulating a European public order which was not, therefore, subject to the principle of reciprocity which is more generally found in the application of international obligations by States*", referring to *Austria v. Italy*, 4 YBECHR 112 (1961). See also Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 37, n° 65 ; Pär Hallström, "The European Union – From Reciprocity to Loyalty", Scandinavian Studies in Law, vol. 39, 2000; pp. 79-88, especially p.82, available at: http://www.scandinavianlaw.se/pdf/39-5.pdf (last accessed on 24 May 2017); Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne*, thesis, Bruylant Bruxelles, 2004, p.297 *et seq.* The principle of reciprocity allows a State to not execute one of its engagements when another party to a treaty does not execute its own.

[16] See Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne, op. cit.* p.65 *et seq*. See also "Convention for the Protection of Human Rights and Fundamental Freedoms", Summary of the treaty, Council of Europe website: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 (last accessed on 24 May 2017): "*Parties undertake to secure these rights and freedoms to everyone within their jurisdiction*".

[17] See Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p.39, n° 68.

[18] Frédéric Sudre, op. cit, p.39, n° 68.

agreement or treaty, to its application by the other party".[19] The Convention is therefore of infra-constitutional but supra-legal force, including on laws adopted subsequent to the Convention[20].

3.3 The relation between law and ethics

Legal instruments might be applied with certain flexibility, depending on the national legal context in which they are integrated, on the manner in which they are written, on their level of detail, on the entity responsible for their enforcement and the prosecution of their violations, and on the stipulated penalties for such violations. Moreover, new technologies may pose novel questions for which there is no incontestable legal answer. In addition, the ECtHR and the CJEU court cases are not always known, these courts did not rule on any IT related privacy issue, and it might be in any case of more value, for a given stakeholder, to choose the less privacy protecting interpretation, when it brings its activities into accordance with law, given the costs and the uncertainty of a trial for any citizen that would challenge this interpretation, above all if he or she needs to recourse to the European or the international Court.

For these reasons, the idea that a full respect for fundamental rights involves considering ethical principles, and not only legal rules, is as old as legal texts protecting individuals, and takes all its meaning when new technologies or new usages emerge, whether or not the notion of "ethics" is explicitly referred to.

There are numerous definitions of ethics and legal ethics. **Within the framework of our study, legal ethics will be defined as "*the ethical principles underlying laws*"**[21]: the intention is to refer to the legislator's spirit, even further to the value system and to the philosophy underlying the legal system[22], and not only to the letter of the legal text. In this sense, ethics "*establishes itself as the natural complement of the conceptualisation of law*"[23]. This leads to interpret the concept of respect for fundamental rights in a protective manner for the individual, taking into account the ECtHR requirements, which must be interpreted in a restrictive way[24].

---

[19] Frédéric Sudre, op. cit, p.39, n° 68. The second part of the text does not receive application because the principle of reciprocity does not apply as regards the ECHR.

[20] Frédéric Sudre, op. cit, p.39, n° 69.

[21] Translated from French: Leslie Sheinman, "Ethique juridique et déontologie", Droit et Société N°36-37/1997, pp. 265-275, available at http://www.persee.fr/doc/dreso_0769-3362_1997_num_36_1_1408 (last accessed on 24 May 2017).

[22] Jean-Claude Rocher, *Aux sources de l'éthique juridique - Les présocratiques*, June 2001, ed. Fac 2000, coll. Reflechir, especially pp. 11-13.

[23] Translated from French, Jean-Claude Rocher, *Aux sources de l'éthique juridique - Les présocratiques*, *op. cit.*, p. 12.

[24] See for example Steven Greer, *The exceptions to Article 8 to 11 of the European Convention on Human Rights,* Human Rights files n°15, Council of Europe publishing, 1997, especially p. 8, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf; Steven Greer, *The margin of appreciation: interpretation and discretion under the European Convention on Human Rights,* Human Rights files n°17, Council of Europe publishing, 2000, especially p. 20 (proportionality); p. 26 (public interest exceptions), http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf; Toby Mendel, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, Council

The study of the legal texts that is proposed in the following sections is therefore, according to the previous definition of legal ethics, also a study of the ethical context, since it is carried out by taking care of interpreting the law in the light of the legislator's spirit[25], of the opinion of legitimate authorities, and of the principles governing the respect of fundamental rights.

Moreover, it has to be noted that legal instruments themselves give increasing prominence to ethics, and that, as a consequence, some past or current ethical behaviours may become future legal explicit obligations. For example, in order to promote respect for ethical principles protecting privacy, two instruments have been gradually developed and recognised: privacy impact assessments[26] and the concept of privacy by design. As analysed in Section 4.2.3.3.13 of the current report, both these instruments become mandatory for data controllers in the new EU legislation on the protection of personal data[27].

3.4 Identification of fundamental rights that might be impacted by the MANDOLA outcomes

It is difficult to ascertain that all the fundamental rights at stake and all the precise risks these rights incur have been identified before the performance of an impact assessment, which is the object of task and deliverable D2.4, in the MANDOLA project. However, such an assessment implies in turn to identify legal constraints, as one of the preliminary steps of its performance. Being an iterative process, the impact assessment might lead in the future to identify additional freedoms at stake, which will be in turn analysed as a complement to the current study.

This first identification of fundamental rights at stake will differentiate between each category of MANDOLA actions, since impact on these rights might be different depending on the action under consideration.

3.4.1 Analysis of the legal prohibitions of hate speech in ten EU Member States, and formulation of recommendations in this regard

An analysis of issues raised by current legal prohibitions might lead to recommend a lower or a higher prohibition of certain kind of behaviours, or a different formulation of these

---

of Europe, especially p. 3 (strict interpretation of the test for freedom of expression restrictions), https://rm.coe.int/16806f5bb3; Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, especially p. 37 (strict interpretation of the test for private life restrictions), www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (URLs last accessed on 12 May 2017).

[25] Especially through analysing, where necessary, the debates that have taken place before the relevant Parliament or, where available, the explanatory statement or report which accompanies the law involved.

[26] See for instance Roger Clarke, "Privacy Impact Assessments", 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 24 May 2017): "*A PIA (…) considers the impacts of a proposed action, and is not constrained by questions of whether the action is already authorised by law. Moreover, to the extent that relevant codes or standards exist, it does not merely accept them, but considers whether they address the public's needs*".

[27] In addition, privacy impact assessments and the notion of privacy by design are analysed more extensively in the MANDOLA deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 11 July 2017.

prohibitions. It might also lead to recommend particular measures in order to ensure the effectiveness of one given prohibition.

In this sense, these recommendations might directly impact the freedom of speech, and its components[28] or corollaries[29] which are the freedom of information and the freedom to communicate. It might also impact the freedom of assembly[30], the right to non-discrimination, the freedom of private life (by preventing people to exchanging and being in touch between themselves[31]), and eventually the protection of personal data (that might be in certain cases more widely collected or accessed, as a consequence of the existing prohibition and its enforcement). In case of action against an illegal content or its supposed perpetrator, this action might also impact the freedom of movement (online or offline), the freedom to conduct a business (in case a website or webpage would be blocked or removed), and, in case of inappropriate action, the presumption of innocence and the right to a fair trial.

3.4.2 Creation of information to be provided to Internet users (awareness) and other stakeholders (best practices and recommendations)

The information to be provided might firstly induce censorship or self-censorship reactions, which might directly impact the freedom of speech, the freedom of assembly, and the freedom of private life (by preventing people to exchanging and being in touch between themselves, which inter alia contributes to their personal development"[32]).

The information to be provided might also induce harmful practices, and impact this way the right to the integrity of the person and his or her right to liberty and security.

The information to be provided might also generates more reports to ISPs or to law enforcement services, which might impact the freedom of speech, the freedom of assembly, the freedom to conduct a business, the right to private life, the protection of personal data

---

[28] See article 10 of the European Convention on Human Rights: "*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers*". Freedom of media is a corollary: see for example the Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, recital n°1, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb844 (URLs last accessed on 24 May 2017).

[29] See for ex. the judgement of the Paris court of appeal (CA Paris), 15/05/1970, conclusions of Mr. Advocate General (Avocat Général) Cabannes, D. 1970 (Dalloz 1970), p. 466.

[30] See for ex. Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa; Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb844 (URLs last accessed on 31 May 2017).

[31] See below Section 4.1.

[32] ECtHR, 3rd Sect., 25 September 2001, *P.G. and J.H. v. the United Kingdom*, appl. n°. 44787/98, §56, http://hudoc.echr.coe.int/eng?i=001-59665, referring to ECtHR, ch., 22 February 1994, *Burghartz v. Switzerland*, §24, Series A, n° 280 B, p. 28, http://hudoc.echr.coe.int/eng?i=001-57865. See also ECtHR, 4th Sect., 29 April 2002, *Pretty v. The United Kingdom*, appl. n° 2346/02, §61, http://hudoc.echr.coe.int/eng?i=001-60448, referring to the same judgment (URLs last accessed on 12 May 2017).

(that might be in certain cases more widely collected or accessed, as a consequence of the report), the freedom of movement and, in case of inappropriate action, presumption of innocence and the right to a fair trial.

3.4.3 Creation of a dashboard that will enable to monitor impersonally the spread of hate speech

Such a dashboard might firstly threaten the right to private life and the right to personal data protection, depending on the information it shows or drives to collect.

Should this dashboard give a mistaken vision of the situation, the rights that might be impacted include the right to receive (truthful[33]) information, and, in case it would lead to mistaken public policies (and therefore to measures that would limit freedoms without being necessary, legitimate and proportionate), the freedoms of expression and to receive and impart information, the freedom of assembly, the freedom of private life (by preventing people to exchange and to be in touch between themselves), and eventually the protection of private life and personal data (that might be in certain cases more widely collected or accessed), the freedom of movement, the freedom to conduct a business, the right to non-discrimination, and even presumption of innocence.

3.4.4 Development of mechanisms that will enable Internet users to report hate speech

Such mechanisms might lead to the communication, to applications, hotlines and/or LEAs, of direct and indirect personal data relating to the potential victim, to the potential perpetrator, to the author of the report, and potentially to other persons. These data might also be further processed. These mechanisms might therefore lead, primarily, to a limitation of the rights to privacy and to personal data protection.

The existence and use of such mechanisms might also lead to self-censorship, to private censorship of contents provided by other persons, and even to the opening of a proceeding. In this respect, the rights that are likely to be limited include the right to private life, the freedom of expression, the freedom of assembly, the freedom to conduct a business, the freedom of movement, the right to non-discrimination, and, in case of inappropriate action, the rights to presumption of innocence and to liberty and security.

In case of malfunction resulting in a damage caused to the user's device, such mechanisms might also limit the freedom of private life, the freedom to communicate and the freedom to assembly.

[33] In the sense of “informative”, in order to give consistency to the right to be informed: see below Section 4.2.2. of the current report.

4 Legal basis and scope of the fundamental rights at stake

The implementation of adequate safeguards during research and in relation to the MANDOLA outcomes requires understanding the notion and the scope of protection of fundamental rights that might be impacted.

The current section will therefore analyse the right to private life, the right to personal data protection, the right to freedom of expression, the right to presumption of innocence and related rights, the right to non-discrimination, the right to freedom of assembly, the freedom of movement, the right to liberty and security, and the right to conduct a business. However, taking into account the necessary limits of the current study, particular emphasis will be mainly put on the three first of these rights, and in a lesser extent on the two following ones, since they appear to be the ones that might be the more impacted by measures aiming at combatting illegal hatred.

4.1 The right to privacy or to private life

Understanding the right to private life requires addressing the protecting legal instruments of this right, the notion of private life, and the nature and extent of the private life protection[34].

4.1.1 Legal instruments protecting privacy or private life

The right to private life or privacy, and more exactly, in the continental European legal tradition[35], the right to respect for private and family life, is protected by several legal instruments. At the international level, it is notably declared by Article 12 of the United Nations Universal Declaration of Human Rights[36], Article 17 of the International Covenant on Civil and Political Rights, and Article 8 of the European Convention on Human Right (ECHR). At the European level, it is protected by Article 7 of the EU Charter of Fundamental rights (EUCFR). At the national levels, the right to respect for private and family life is moreover protected by several Constitutions[37].

---

[34] Some elements of the following discussion are based or coming from Estelle De Marco *in* Estelle De Marco *et al*., Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.1, available at https://www.epoolice.eu/. See also Estelle De Marco *in* C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, Chapters 6 and 7, available at http://www.aconite.com/blocking/study (French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ - URL last accessed on 12 May 2017).

[35] Regarding the difference between the continental European tradition and the Anglo-American legal tradition, see Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*, Springer, 15 November 2007, p. 113.

[36] This declaration, adopted by the General Assembly of the United Nations on 10 December 1948 "*is no more than a recommendation and thus is non-legally binding* ". It aims nevertheless *"to express an ideology shared by all humankind"*: Frédéric Sudre," La déclaration universelle des droits de l'homme", JCP n° 52, 23 Dec. 1998, act., p. 2 249 (translated from French).

[37] The right to respect for private life is for example protected by article 18 of the Spanish Constitution, and article 11 of the Constitution of Luxembourg. It is also protected by several articles under Title II of the

These texts protect more precisely individuals from arbitrary interference with their private life, family, home or correspondence, and from attacks upon their honour and reputation, at least at the Council of Europe and European Union levels[38].These two levels are of particular interest and will constitute our main focus since the ECHR[39] and the EUCFR[40] are binding for all EU Member States.

4.1.2 The notion of privacy or private life

There are several definitions of the sphere of private life as it is protected by legal instruments[41]. In this respect Daniel J. Solove considered that privacy is a "concept in disarray", a notion that "suffers from an embarrassment of meanings".[42]

This situation seems primarily due to the silence of these legal instruments in relation to the content of privacy, and to the difference or at least apparent difference between judicial and philosophic approaches, which both lead to various doctrinal interpretations.

In this context, four doctrinal main approaches might be differentiated[43]. The first one consists of endeavouring to identify the boundaries of private life through the identification of its elements of content (4.1.2.1). The second one consists of breaking privacy into several "categories" or "dimensions" depending on the context of the privacy exercise, most of these categories enabling to figure out their respective elements of content (4.1.2.2). The

---

Romanian Constitution adopted in 1991 (inter alia, article 26 states "*Public authorities shall respect and protect intimacy, family and private life*"; article 28 covers the secrecy of letters and communications). In France, the right for private is protected by the French Constitutional Council on the basis of articles 2 and 4 of the French Human and Citizens Rights Declaration of 1789, which is included in the so-called French "constitutionality bloc" (see for ex. Conseil constitutionnel, Decision n° 2004-492 DC, 2 March 2004, J.O. 10 March 2004, page 4 637, Recital n° 4).

[38] The EUCHR has the same meaning and scope as the ECHR, and the ECtHR organises the protection of honour and reputation under article 8. See for instance ECtHR, ch., 21 September 1994, *Fayed v. the United Kingdom*, appl. n°17101/90, http://hudoc.echr.coe.int/eng?i=001-57890; ECtHR, 2nd sect., 29 June 2004, *Chauvy and Others v. France*, appl. n° 64915/01, §70; http://hudoc.echr.coe.int/eng?i=001-61861; ECtHR, ch., 20 October 2005, *Gunnarsson v. Iceland*, appl. n° 4591/04, http://hudoc.echr.coe.int/eng?i=001-71525 (URLs last accessed on 12 May 2017). For all these references, see Key case-law issues, the concepts of "private and family life", European Court of Human Rights, 24/01/2007.

[39] The 28 member countries of the European Union are also member countries of the Council of Europe and have accessed or ratified the European Convention on Human Rights. Moreover, the European Union is currently also acceding to the Convention.

[40] The charter has the *"same legal value as the Treaties"*: article 6 TEU.

[41] In relation with this section see Estelle De Marco *in* Estelle De Marco *et al.,* Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.1.2 (with the contribution of Javier Valls Prieto in what regards Spain), https://www.epoolice.eu/ (last accessed on 24 November 2016).

[42] Daniel J. Solove, « A taxonomy of privacy », University of Pennsylvania Law Review, vol. 154, n° 3, Jan. 2006, http://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf (last accessed on 12 May 2017).See also Daniel J. Solove, Understanding privacy, Harvard University Press, 2008, esp. p.1 *et seq*.

[43] For an overview of different conceptions of privacy, including its deny, see Judith DeCew, "Privacy", The Stanford Encyclopedia of Philosophy (Spring 2015 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2015/entries/privacy/ (last accessed on 12 May 2017).

third one consists of breaking privacy into rights that are implied by the protection of privacy more generally, whatever are the elements of information covered by privacy, and therefore without pre-empting a conclusion on the identification of these elements (4.1.2.3). The fourth approach consists of a negative definition of privacy, in relation to third parties' rights (4.1.2.4).

4.1.2.1 Identification of the boundaries of private life through the identification of its elements of content

Traditionally, a large doctrine considers private life as being composed of several circles. Each of these circles is composed of certain elements of information or even of certain freedoms. The more the protected circles are numerous, or the more the protected circles contain information or freedoms, the more privacy is considered to be protected. In this latter case, the conception of privacy is called "extensive", in contrast to the "restrictive" conception. Alternatively, some of these circles are considered to be protected in any case, while certain other are only protected in certain circumstances or toward certain persons.

For example[44], in France, Prof. François Terré has identified several private life circles protected by French judges[45]. At the centre of private life, the circle of "personal life" contains "*data related to identity, to racial origin, to physical or mental health, to one's character or morals*"[46]. Genetic information constitutes another circle, and a larger circle includes data related to "*sentimental, conjugal, extra-conjugal and familial life*", to *"friendly relations*", to "*the participation in private assembly*"[47]. The domicile[48] and private correspondence[49] are also protected circles of private life. This French conception of private life is considered to lie amongst the restrictive ones[50].

Holders of the most extensive view of privacy agree to understand the concept as being the "*right to be left alone*"[51], which refers to "*the right of everyone to take decisions at his own*

[44] For other national examples, see for instance Estelle De Marco *et al.,* Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, available at https://www.epoolice.eu/, Section 3.

[45] François Terré, "La vie privée", *in La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tomes 3, 4 et 5, Cahier des sciences morales et politique, PUF, 1re éd., janv. 2002, p. 135. See also Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 41 *et seq*.

[46] François Terré, "La vie privée", *op. cit*., page 138.

[47] François Terré, "La vie privée", *op cit*., page 139. Estelle De Marco, *L'anonymat sur Internet et le droit*, *op cit*, n° 41.

[48] See for ex. a decision of the French Supreme Court: Cass. Civ. 3ème, 25 February 2004, Bull. civ. III, n° 41, p. 38.

[49] See for instance the so called « Nikon » French Court case, Cass. soc., 2 October 2001, Bull. civ. V, n° 291, p.233.

[50] Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p.27 *et seq*.

[51] Stéphane-Dimitri Chupin, *La protection de la vie personnelle délimitée par les frontières des sphères privées et publiques*, thesis, Université Paris I, 2002, p. 32; Samuel D. Warren and Louis D. Brandeis, "The right to privacy", Harvard Law Review, vol. IV, 15 Dec. 1890, n°5. For an history of privacy including comments on S. Warren and L. Brandeis conception of privacy, see Ahti Saarenpää, "Perspectives on privacy", in Ahti Saarenpää, *Legal privacy*, LEFIS Series, 5, Prensas Universitarias de Zaragoza, p. 20

discretion into his zone of private life"[52], or to the right to an opportunity to shape one's own life, with minimal outside interference[53].

Between the two afore-mentioned conceptions, the European Court of Human Rights (ECtHR) considers privacy as a "*broad term*", which is "*not susceptible to exhaustive definition*"[54], and which cannot be limited to "*an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle*"[55]. The ECtHR therefore includes for instance, within the privacy sphere as protected by texts, the "*right to identity*[56] *and personal development*"[57], and the right, to a certain degree, "*to establish and develop relationships with other human beings*"[58], the right to *"self-determination and personal autonomy"*[59], *"the physical and*

(http://puz.unizar.es/detalle/898/Legal+privacy-0.html), available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf (last accessed on 12 May 2017); François Rigaux, "Les paradoxes de la protection de la vie privée", *in La protection de la vie privée dans la société d'information*, *op. cit*., p. 37, quot. p. 41.; González Rus, J.J. "Capítulo 14. Delitos contra la Intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio (1)" in Morillas Cueva, L. *Sistema de Derecho Penal Español. Parte Especial*, 2011, p.287. The latter reference comes from Javier Valls Prieto and can be also found in Estelle De Marco *et al.,* Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, available at https://www.epoolice.eu/, Section 3.

[52] According to the Supreme Court of the United States in a decision of 1965. Translated from French. Pierre Tabatoni, "Vie privée : une notion et des pratiques complexes", in *La protection de la vie privée dans la société d'information*, under the direction of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, Oct. 2000, p. 3, quotation p. 4.

[53] Formula from Prof. Stig Strömholm according to Advocate General Cabannes in conclusions sous CA Paris, 15 mai 1970, D. 1970, jurisp. p. 466, quot. p. 468. Prof. Stig Strömholm conception of privacy is also mentioned by Alexandre Maitrot de la Motte, "Le droit au respect de la vie privée", in *La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tome 3, 4 et 5, Cahier des sciences morales et politique, PUF, Jan. 2002, p. 271, and by Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 329.

[54] ECtHR, 4th Sect., 28 January 2003, *Peck v. United Kingdom*, appl. n° 44647/98, §57, http://hudoc.echr.coe.int/eng?i=001-60898. See also ECtHR, ch., 16 December 1992, *Niemietz v. Germany*, appl. n°13710/88, §32, http://hudoc.echr.coe.int/eng?i=001-57887: *"The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life"* (URLs last accessed on 12 May 2017).

[55] ECtHR, *Niemietz v. Germany*, *op. cit*. §29.

[56] The ECtHR adds that article 8 of the convention protects "*aspects of an individual's physical and social identity"* in ECtHR, 1st Sect., 7 February 2002, *Mikulić v. Croatia*, application no. 53176/99, §53, http://hudoc.echr.coe.int/eng?i=001-60035 (last accessed on 12 May 2017).

[57] ECtHR, 3rd Sect., 25 September 2001, *P.G. and J.H. v. the United Kingdom*, appl. n°. 44787/98, §56, http://hudoc.echr.coe.int/eng?i=001-59665, referring to ECtHR, ch., 22 February 1994, *Burghartz v. Switzerland*, §24, Series A, n° 280 B, p. 28, http://hudoc.echr.coe.int/eng?i=001-57865. See also ECtHR, 4th Sect., 29 April 2002, *Pretty v. The United Kingdom*, appl. n° 2346/02, §61, http://hudoc.echr.coe.int/eng?i=001-60448, referring to the same judgment (URLs last accessed on 12 May 2017).

[58] See the judgments mentioned in the previous note and ECtHR, *Niemietz v. Germany*, *op. cit*., §32; Relating to the non-exclusion of "*the right to establish and develop relationships with other human beings*" and of "*activities of a professional or business nature*", see also the judgment ECtHR, gr. ch., 16 February 2000, *Amann v. Switzerland*, appl. n° 27798/95, §65, http://hudoc.echr.coe.int/eng?i=001-58497 (last accessed on 12 May 2017).

psychological integrity of a person"[60], "*professional and business activities*"[61], and correspondence[62], which includes notably letters[63], telephone calls and conversations[64], including information relating to them such as their date or the number dialed[65], pager messages[66], professional correspondence[67], correspondence intercepted in the course of business or from business premises[68], and electronic communications (including the right for an individual to control "*information derived from the monitoring of (his or her) personal Internet usage*"[69]). Personal data are also protected[70] and the ECtHR considers especially that both the storing and the release by a public authority of information relating to an

[59] Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, p. 12, available at: www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (last accessed on 12 May 2017); see also for instance the case ECtHR, *Pretty v. The United Kingdom*, *op. cit.,* §§ 61 and 67.

[60] Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, *op. cit*., p. 22, referring to ECtHR, gr.ch., 16 December 2010, *A, B, and C v. Ireland*, application n° 25579/05, http://hudoc.echr.coe.int/eng?i=001-102332; see also ECtHR, ch., 26 March 1985, *X and Y v. the Netherlands*, appl. n°8978/80, § 22, http://hudoc.echr.coe.int/eng?i=001-57603 (URLs last accessed on 12 May 2017).

[61] ECtHR, *Niemietz v. Germany*, *op. cit*., §28 and 29; See Pierre Kayser, op cit, page 43 and 44 and footnote n° 158. Before the ECtHR has ruled on this subject, the Court of Justice of the European Union stated that the need for a protection of legal persons' private sphere of activities "*must be recognized as a general principle of Community law*": judgment of 21 September 1989, *Hoechst v. Commission*, joined cases 46/87 and 227/88, European Court Reports 1989, pp. 2859-2924.

[62] See for instance Commission, plen., 27 February 1995, *B.C. v. Switzerland*, Application n°21353/93, http://hudoc.echr.coe.int/eng?i=001-2039; ECtHR, ch., 25 March 1983, *Silver and others v. the United Kingdom*, appl. n°5947/72, § 84, http://hudoc.echr.coe.int/eng?i=001-57577 (URLs last accessed on 12 May 2017).

[63] See for instance ECtHR, *Silver and others v. the United Kingdom*, *op. cit.* §84.

[64] See for instance ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §41, http://hudoc.echr.coe.int/eng?i=001-57533; ECtHR, ch., 16 December 1992, *Niemietz v. Germany*, appl. n°13710/88, §32, http://hudoc.echr.coe.int/eng?i=001-57887 (URLs last accessed on 12 May 2017).

[65] ECtHR, 3rd Sect., 25 September 2001, *P.G. and J.H. v. the United Kingdom*, appl. n°. 44787/98, http://hudoc.echr.coe.int/eng?i=001-59665 (last accessed on 12 May 2017).

[66] ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, http://hudoc.echr.coe.int/eng?i=001-60696 (last accessed on 12 May 2017).

[67] ECtHR, *Niemietz v. Germany*, *op. cit.*, §32.

[68] ECtHR, ch., 25 March 1998, *Kopp v. Switzerland*, appl. n°23224/94, §50, http://hudoc.echr.coe.int/eng?i=001-58144; ECtHR, ch., 25 June 1997, *Halford v. the United Kingdom*, appl. n°20605/92, §§ 44-46, http://hudoc.echr.coe.int/eng?i=001-58039 (URLs last accessed on 12 May 2017).

[69] See ECtHR, 4th Sect., 3 April 2007, *Copland v. the United Kingdom*, appl. n° 62617/00, § 41, http://hudoc.echr.coe.int/eng?i=001-79996 (last accessed on 12 May 2017): "*According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8 § 1 (see Halford, op cit, § 44 and Amann v. Switzerland [GC], no. 27798/95, § 43, ECHR 2000-II). It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage*". On this issue and the previous ones, see Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, p. 32, available at: www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (last accessed on 12 May 2017).

[70] ECtHR, gr. ch., 16 February 2000, *Amann v. Switzerland*, appl. n° 27798/95, §65, http://hudoc.echr.coe.int/eng?i=001-58497 (last accessed on 12 May 2017).

individual's private life amounts "*to an interference with his right to respect for private life*[71]", no matter how the stored information will be used[72] and particularly within the context of "*surveillance methods resulting in masses of data collected*"[73]. More generally, "*mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*"[74].

4.1.2.2 Breaking privacy into several "categories" or "dimensions" depending on the context of the privacy exercise

Other legal authors distinguish several privacy categories, which is perfectly illustrated by the research consortium of the PIAF project[75]: "*For example, Clarke considers four conventional yet overlapping categories: privacy of personal information, of a person, of personal behaviour, and of personal communications.*[76] *For the PRESCIENT project, the research consortium has identified seven types of privacy: of a person, of thought and feelings, of location and space, of data and image, of behaviour and action, of communications, and of association, including group privacy*[77] *Solove argued that the conceptions of privacy could be grouped in six categories: the right to be let alone, limited access to the self, secrecy, control over personal information, personhood and intimacy.*[78] *Rössler has analysed three dimensions of privacy: decisional privacy, informational privacy, and local privacy (i.e. privacy of the household)*".[79] For his part, Ahti Saarepää identifies "*at least (…) eleven main core areas*" of privacy: physical privacy, spatial privacy, social privacy, media privacy, anonymity, privacy in the processing of personal data, ownership of

---

[71] ECtHR, ch., 26 March 1987, *Leander v. Sweden*, appl. n°9248/81, §48, http://hudoc.echr.coe.int/eng?i=001-57519; See also ECtHR, gr.ch., 4 May 2000, ECtHR, *Rotaru v. Roumania*, appl. n°28341/95, §45 *et seq,* http://hudoc.echr.coe.int/eng?i=001-58586 (URLs last accessed on 12 May 2017).

[72] ECtHR, gr.ch., 16 February 2000, *Amann v. Switzerland, op. cit.* §69; See also (rel. to phone calls) ECtHR, ch., *Kopp v. Switzerland, op.cit.* §53.

[73] ECtHR, 4e sect., 12 janvier 2016, *Szabó and Vissy v. Hongrie*, appl. n°37138/14, §68, http://hudoc.echr.coe.int/eng?i=001-160020 (last accessed on 18 May 2017).

[74] European Court of Human Rights, Factsheet, « Protection of personal data », Press Unit, April 2017, p. 1, available on the Council of Europe website: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last accessed on 12 May 2017).

[75] Paul De Hert, Dariusz Kloza, David Wright and all., Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.13, available at http://www.piafproject.eu/Deliverables.html (last accessed on 12 May 2017).

[76] Clarke, Roger, *What's Privacy'?*, 2006, http://www.rogerclarke.com/DV/Privacy.html (last accessed on 12 Mat 2017).

[77] Gutwirth, Serge, Michael Friedewald, David Wright, Emilio Mordini et al., Legal, social, economic and ethical conceptualisations of privacy and data protection, Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment], p. 8, http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf (last accessed on 12 Mat 2017). See also Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2012, pp. 3-32.

[78] Solove, Daniel J., "Conceptualizing Privacy" *California Law Review*, Vol. 90, 2002, p. 1087.

[79] Rössler, Beate, *The Value of Privacy*, Polity Press: Cambridge, 2005, p 86.

information, right to be assessed in the proper light, patient privacy, privacy in working life, and communicative privacy[80]. In the context of Ambiant intelligence, Antoinette Rouvroy details for her part five aspects of privacy which are spatial, informational, emotional, relational and communicational privacy[81].

Links with this conception of privacy and the one exposed in the previous section can be clearly made. For example, the protection by the ECtHR of the right for an individual to control "*information derived from the monitoring of (his or her) personal Internet usage*"[82], belongs to the "informational privacy" identified by Antoinette Rouvroy[83] and other authors. However, they try to identify large categories of behaviours or contexts rather than enumerating the precise information pieces or actions they cover, and in this sense present the risk to not ensure that the entire category is protected by courts.

4.1.2.3 Breaking privacy into rights that are implied by the protection of privacy, without regard to their elements of content

Beside the afore-mentioned conceptions of privacy, Prof. Pierre Kayser[84] divides private life into two privacy spheres or dimensions which can be referred to as the “secrecy of private life” and the “freedom of private life”.

The secrecy of private life is the "opaqueness for others of the personal and family life". It notably includes the secrecy of communications, the secrecy of relationships built up with third parties, the right to be forgotten, and the secrecy of one person's image and voice[85]. The freedom of private life is defined as "the power, for a person, to take the decisions that seem to her the bests for this part of her life"[86], as a "general freedom which includes several particular freedoms", which may be described as physical (as the physical freedom, the freedom of movement) or as moral (as the freedom of belief)[87]. It notably includes the release from the home "to develop one's physical, intellectual, moral and spiritual personality"[88], the freedom of movement on the Internet, the freedom to make decisions, to

[80] Ahti Saarenpää, *Legal privacy*, Lefis series 5, PUZ/LEFIS, 2008, *op. cit.,* pp. 27 *et seq*.

[81] Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 25. This publication is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (last accessed on 12 May 2017).

[82] ECtHR, 4th Sect., 3 April 2007, *Copland v. the United Kingdom*, appl. n° 62617/00, § 41, http://hudoc.echr.coe.int/eng?i=001-79996 (last accessed on 12 May 2017). See footnote n°69.

[83] See, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", *op.cit*. The author considers that informational privacy is an area where the scope of the right to privacy and of the right to personal data protection may intersect.

[84] Pierre Kayser, *La protection de la vie privée par le droit*, PU d’Aix-Marseille/Economica, 3rd ed., 1995, p. 12. On the secrecy of privacy, see also M. Rudinsky, Civil Human Rights in Russia: Modern Problems of Theory and Practice, Transaction Publishers, 2008, IBSN 978-0-7658-0391-7.

[85] See Estelle De Marco, *L’anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n°s 41, 107, 109, 114, 122, 135, 137, 147, 162, 171-172, 332.

[86] Translated from French. Pierre Kayser, *La protection de la vie privée par le droit*, *op. cit*. p. 11; see also Estelle De Marco, *L’anonymat sur Internet et le droit*, *op cit* p.99 *et seq*.

[87] Pierre Kayser, *op. cit.*, p. 344 and p. 12.

[88] Pierre Kayser, précité, p. 12. See also Estelle De Marco, *L’anonymat sur Internet et le droit*, *op. cit*. n° 133 *et seq*.

make choices, notably regarding purchased goods and services[89], to communicate these choices to third parties, to open the doors of one's own private life to certain persons and to close these doors to other people[90]. Freedom of private life underlies the right to private life, since it enables to create the content to the private sphere[91].

The secrecy and the freedom of private life may therefore be seen as two dimensions of private life, in which the other categories of privacy, analysed above, may take place.

4.1.2.4 Negative definition of privacy, in relation to third parties' rights

The above mentioned conceptions of privacy, which give to the latter a more or less extensive content without spelling out all of the private life details, do not allow the definition of the precise scope of the notion with certainty. In this respect, Daniel J. Solove considers that the concept is "*far too vague (…) to guide adjudication and law making, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests*"[92].

The reasons for this situation seem to lie in a confrontation of two notions which bounds are, at first sight, rather different:

- A philosophical or "emotional"[93] notion of privacy, which in general tends to see or is susceptible to include each element or most elements of one's personal life as "private", either when the person involved so decides[94], or more generally, because it is "desirable"[95], or because this element of personal life is simply an element that

[89] See the French Supreme Court decision: Cass. soc., 22 Jan. 1992, Bull. civ. V, n° 30.

[90] See for instance Emmanuel Dreyer, "Le respect de la vie privée, objet d'un droit fundamental", Com. com. élec., n° 5, May 2005, I, 18.

[91] Regarding this paragraph, see Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit*. n° 147-148.

[92] Daniel J. Solove, « A taxonomie of privacy », University of Pennsylvania Law Review, vol. 154, n° 3, Jan. 2006, http://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf (last accessed on 12 May 2017).See also Daniel J. Solove, Understanding privacy, Harvard University Press, 2008, esp. p.1 *et seq*.

[93] Mats G. Hansson, *The Private Sphere, An Emotional Territory and Its Agent*, Springer, 2008.

[94] The notion of privacy is indeed extremely subjective. See for instance Mats G. Hansson, *op. cit*. p. 1 and p. 9 (according to the autor, "*the boundaries defining the private sphere vary from individual to individual*"); Estelle De Marco, *Privacy and Personal Data Protection: Legal Context and Social Perception*, FIA 2011 Budapest, 18 May 2011, session "Economics of Privacy", http://www.future-internet.eu/home/future-internet-assembly/budapest-may-2011/session-i3-the-economics-of-privacy.html. See also Caroline Lancelot Miltgen, "Vie privée et Internet : influence des caractéristiques individuelles et situationnelles sur les attitudes et les comportements des internautes face à la collecte des données personnelles", cahier de recherche DMSP n° 317 et actes du congrès AFM Tunis 2003, http://halshs.archives-ouvertes.fr/docs/00/45/78/67/PDF/C. Lancelot Miltgen Vie privee et Internet AFM 2003 hal.pdf; Caroline Lancelot Miltgen and Claire Gauzente, "Vie privée et partage de données personnelles en ligne : une approche typologique", cahier de recherche DMSP n° 356, April 2006, http://basepub.dauphine.fr/handle/123456789/4216; Caroline Lancelot Miltgen, "Dévoilement de données personnelles et contreparties attendues en e-commerce : une approche typologique et interculturelle", Système d'information et management (SIM), vol. 15, n° 4, Dec. 2010, pp. 45-91. Ruth E Gavinson quoting Edward Shil's theory, in "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, particularly p.427, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (URLs last accessed on 12 May 2017).

[95] Ruth E Gavinson, "Privacy and the limits of law", *op. cit.*, p 425.

would be private if the person involved would be inaccessible to others, within the framework of a "neutral" concept of privacy[96];

- A judicial notion of privacy, which varies across territories, and which tends to limit the notion to a smaller nucleus of protected elements, particularly with the objective of respecting the rights of third parties and of respecting the boundaries of the public sphere which is a place for exchange and for the exercise of other freedoms[97]. The contours of private life cannot, in such circumstances, be closely defined by judges, particularly because a lot of public freedoms - whose legal protection should allow a public exercise - are exercised in the secrecy of private life, this being sometimes the price to pay for the protection of the individual[98]. In consequence, judges and courts refrain from giving too restrictive boundaries to privacy, in order to make it possible, in a casuistic manner, to provide refuge for certain secrets or certain individual freedoms[99] in this protected private zone[100].

However, we notice that these two approaches and the analyses that support them have a point in common: the existence of limits to privacy, due to the interaction of the individual with others.

For these reasons, several authors consider that privacy must be negatively defined, through the identification of its limits. These limits are the measures that allow pursuing public interests[101] or the defence of third parties rights[102], in addition to the bounds that a person assigns to his or her own privacy sphere[103]. Indeed, each privacy definition seems offering to

[96] Which is Ruth E Gavinson theory: see "Privacy and the limits of law", *op. cit*., p. 428.

[97] On this issue see for instance Hannah Arendt, "Qu'est-ce que la liberté ?" (What is freedom?)*,* in *La crise de la culture*, ed. Gallimard, coll. Folio/essais, Jan. 2000, p. 186 and particularly p. 200. See also Stéphane-Dimitri Chupin, *La protection de la vie personnelle délimitée par les frontières des sphères privées et publiques*, thesis, Paris I, 2002, particularly the section entitled "L'importance de la vie publique dans la cité", p. 75 *et seq*.

[98] See for instance Raymond Aron, *Essai sur les* libertés, ed. Hachette, coll. Pluriel, 1976, p. 215: "*Freedom does not exist without the existence of a sphere where everyone is his own master and make his own decisions*" (translated from French); François Terré, , "La vie privée", in *La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tome 3, 4 et 5, Cahier des sciences morales et politique, PUF, 1st ed., Jan. 2002, p. 135, cit. p. 135: the "*protection of a person's intimate sphere (...) is a way of respecting his or her freedom*" *(translated from Franch)*.

[99] See Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995 p. 12, quoting Marie-Thérèse Meulders-Klein, "Vie privée, vie familiale et droits de l'homme", Rev. intern. dr. comp., 1992, p. 771: "*It is an essential qualitative leap to get from the secret and intimacy protection to the idea that the secret is only the means of protecting individual freedom (…), which is in turn only the means of ensuring the personal achievement of each individual*". See also Alan Westin, *Privacy and Freedom*, Athenum, 1967.

[100] See for instance Advocate General Cabannes, conclusions sous (ie opinion under the Paris Court of Appeal decision) CA Paris, 15 mai 1970, D. 1970, jurisp. p. 466, quotation p. 468: According to the author, French judges appropriately refrain from "*formulating a general definition in an area whose limits are undecided. In each individual case, they simply give an outline that enables giving to private life an assessment that is wide enough to protect the right to live in peace at home*" (translated from French).

[101] On this issue see for example Amitai Etzioni, *The limits of privacy*, Basic Groups, 1999, notably p. 4.

[102] The defence of several public interests and third parties' rights are generally the objectives that enable the limitation of conditional rights according to the ECHR.

[103] Unless prohibited by law, the right to privacy includes the right to choose to not benefit from this protection.

an individual the possibility to interact with third parties and the public sphere[104], and therefore the possibility to authorise these third parties integrating a part of his or her private sphere, even to create rights, for these third parties, over the content of his or her private life. Moreover, this given individual has decided to live in society and therefore has accepted to bow to the general will, thereby authorising certain State's interventions[105].

In this sense, some authors analyse privacy not as a "*secret garden*", in a pure "*geographical conception*"[106], but as a personal zone that must be reconciled with the necessary interactions a person has with others[107], or as a sphere where the individual can do anything that is not prohibited by law[108], which also implies relations with third parties. These conceptions imply that the content of the private sphere is primarily defined in relation to third parties' rights[109], third parties who may be more or less legitimate to control another person's freedom to act or another person's personal information[110].

Prof. Pierre Kayser[111] itself shows that the apparent indecision of the French court of cassation in relation with the content of private life is due to the fact that the court does not

---

[104] See for instance Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*", Springer, 2007, pp. 1 *et seq*.

[105] Jean-Jacques Rousseau, "The social contract", *in* Robert A. Dahl, Ian Shapiro and José Antonio Cheibub, *The democracy MIT Press, 2003,* p.2 *et seq*.

[106] Emmanuel Dreyer, "Le respect de la vie privée, objet d'un droit fondamental", Com. com. élec., n° 5, May 2005, I, 18.

[107] See for example Ruth E. Gavinson, "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (URLs last accessed on 12 May 2017); Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*", Springer, 2007, pp. 2 *et seq*.

[108] See for instance Emmanuel Dreyer, *op. cit*.;

[109] See for instance Florence Deboissy, "La divulgation d'une information patrimoniale", D. *2000, chron. p. 26: "The right to respect for private life is completely directed against others. Its object must therefore be defined in relation to third parties"* (translated from French); José Duclos, *L'opposabilité - Essai d'une théorie générale*, Thesis, LGDJ, 1984, n° 177. See also Ruth E Gavinson, "Privacy and the limits of law", *op. cit*.: "*Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention*" (p. 423); "*The desire not to preempt our inquiry about the value of privacy by adopting a value-laden concept at the outset is sufficient to justify viewing privacy as a situation of an individual vis-a-vis others, or as a condition of life*" (p. 425).

[110] On the legitimacy criterion, see for instance Florence Deboissy, "La divulgation d'une information patrimoniale"*, D. 2000, chron. p. 267: "The debate is (…) about the legitimacy of the control of the information, which special characteristic is to be personal, that is to say representative of a personality. Moreover, such a conception of private life allows forestalling the classical criticism of the theory of rights in the personality, that is to say the confusion between object and subject of law. Indeed, each individual has a prerogative not on himself but on an object that is outside of himself, the information"* (translated from French). On the coexistence of freedoms and personal data in the content of private life, see for instance Ahti Saarenpää, "Perspectives on privacy", available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf p. 21: "*when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone*" (last accessed on 12 May 2017).

[111] Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 350.

characterise the privacy limitation according to the private nature of the concerned element of life, but does characterise it according to the severity of the limitation[112], and, in other words, according to the legitimacy of the limitation brought to the personal sphere of an individual by a third party.

Such a conception of privacy seems also to be close to the concept of "integrity" developed by Mats G. Hansson: this author considers the private sphere as an emotional territory, "*which forms the individual's own sphere of action and experience*", and which "*has developed in the course of evolution in pace with the changes in the individual's conditions of life, brought about by challenges in the natural and social environment*". According to Mats G. Hansson, "*this emotional territory allows a readiness to act along different lines and to maintain a multiplicity of different social relations*". Mats G. Hansson therefore uses the term "integrity" in order "*to capture the fundamental notion of agency involved in an individual's efforts to expand, defend, and, sometimes, give up the private sphere*". Mats G. Hansson adds that "*respect for integrity focuses on the agency of an individual trying to relate the private sphere to an active participation in social and public life*"[113].

Moreover, this possibility to interfere with one's private life is explicitly mentioned by the European Convention and Court of Human Rights, which impose clear restrictions to such interferences, in order to protect individuals against arbitrariness: any interference with the exercise of the right to privacy must be permitted or prescribed by law, must pursue one of the legitimate aims that are exhaustively listed in the convention, and must be necessary and proportionate[114].

4.1.2.5 Conclusion

In the light of the preceding analyses, the more relevant definition of privacy appears to be a negative definition in relation to third parties' rights, applied to the confidentiality and to the freedom of private life. Indeed, this definition encompasses most of the other ones - if not all - and seems consistent with the outcomes of courts' decisions, in addition to be very protective of the right to private life. However, this definition is not exempt from a dependency on ways and morals of the time, and must always be confronted to these values where the purpose is to identify precisely the elements that must be seen as belonging to the protected private sphere of a given individual.

4.1.2.5.1 Negative definition of privacy, applied to its secrecy and freedom

The definition of privacy through its limits, and more precisely the rights of other, either defined by law in order to pursue the public interests or the defense of third parties rights, or defined by the concerned person him or herself in order to build relationships with other human beings, seems to be the more relevant definition, if put into perspective with the identification of the two crucial aspects of privacy which are the "secret" or confidentiality of

[112] Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 105.

[113] For all quotations see Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*, Springer, 2008, p. 3.

[114] For further details, see the following section.

private life on the one hand, and the "freedom" of private life on the second hand, two aspects that appear clearly in each conception of privacy that has been studied above.

Under such an approach, private life (as protected by law) might be more precisely defined as being composed of two groups of elements[115]:

- Pieces of information related to personal life over which third parties have no legitimacy of control, control that may for instance consist of knowing, collecting, using, repeating or publishing the information;
- Freedoms exercised in the personal sphere (in other words the freedom of privacy), with which third parties must not interfere, and which may themselves be the subject of personal information.

In that definition,

- The notion of "personal information" refers to any information related to someone's life, that is to say to any "objective" information that would be associated with a specific "subject", in other words with a specific individual, the latter being directly or indirectly identifiable;
- The notion of "third parties" includes natural persons and legal persons, including States;
- The notion of "legitimacy" refers to some sort of "right"[116] enabling third parties to penetrate another person's personal sphere, right that must be prescribed by law, and whose exercise must be restricted to measures that are necessary and proportionate, or right whose boundaries may be determined by the person whose private life is concerned, when law does not render such consent ineffective.

Private life as protected by law seems therefore include as many spheres as elements, around a designated individual, and each of these spheres incorporate a more or less extensive group of individuals who are legitimate to be in there in a certain manner and for certain reasons, knowing that these legitimate reasons may disappear over time[117]. Elements of each of these spheres may have been lived electronically, or lived offline, but they are always likely to be communicated on the Internet or on another network. In the centre of private life, several spheres are particularly related to marital, emotional and sexual life, to health and body's intimacy, and are generally legitimately accessible to only an infinitesimal minority of persons. This set of spheres constitutes a nucleus which is protected

---

[115] On this definition see Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), especially n° 33 et seq., n°109 et seq.; Estelle De Marco *in* Estelle De Marco et al., Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3, available at https://www.epoolice.eu/.

[116] Such a "right" is not necessarily a subjective right, in other words a right that is binding on third parties and whose respect or entitlement may be requested before a court. It may be only a freedom in the form of an authorisation, even an exception, which justifies the presence of a person in the private zone of another individual (presence which is therefore not constitutive of a fault). Such right, freedom or exception may moreover be limited in time.

[117] See for example ECHR, 2nd sect., 18 May 2004, *Editions Plon v. France*, appl. n° 58148/00, http://hudoc.echr.coe.int/eng?i=001-61760 (last accessed on 12 May 2017); Légipresse n° 215, Oct. 2004, III, p. 173, annotation by Camille Bauer p. 176.

extensively, almost systematically, since it is protected against the overwhelming majority of third parties. Other spheres are related to the other elements of the individual's personal life, and include a larger or smaller number of third parties who are allowed either to be informed, or, for instance, to collect these elements within the framework of the performance of a contract. The protection of certain elements belonging to the extensive conception of privacy only applies in regard of a lower number of people who are illegitimate to penetrate in the sphere that include these elements. Finally, private life is not protected against disclosure when, for instance, everyone has a legitimate interest in accessing to information, which has been held by the French County Court of Nanterre, France, with regard to a television presenter's capillary evolution[118]. However, an absence of protection against disclosure does not mean that other types of information processing are allowed.

4.1.2.5.2 A definition that remains dependent on ways and morals of a time

As seen above, The notion of legitimacy of third parties, in the above-mentioned definition, stays dependent on ways and morals of a time, since outside any legal explicit authorisation to interfere with the sphere of privacy of another person, or without explicit authorisation from this person, their legitimacy will depend on what belongs to their own sphere of "freedom", which authorises to do everything that is not prohibited[119], subject to (generally civil) liability in case of fault[120] or abuse of right[121]. The fault or abuse of right is generally assessed in the light of what it is common to do or to not do in certain circumstances and of what it is admitted in terms of being at a certain place at a certain moment, or of behaving in a certain manner in certain circumstances[122]., or even of what should or not contribute to a debate of public interest[123]. In this regard the application of the requirements prescribed in

---

[118] TGI Nanterre (French County Court of Nanterre), 1st ch. A, 15 July 1999, D. 2000, n° 26, somm. com. p. 272, obs. Christophe Caron. On this analysis as a whole, see Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit*. n°116.

[119] This principle is part of the definition of freedom and is proclaimed by the Constitutions of several countries including France (art. 4 of the Human and Citizen Rights Declaration of 1789: "*Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law*" - official English translation at translation at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/constitution/declaration-of-human-and-civic-rights-of-26-august-1789.105305.html). In the criminal area, it is included in the principle "*nulla poena sine lege*" protected by Art. 7 of the ECHR (see Section 4.4.2 of the current study).

[120] Legal actions, in case of fundamental right violation, are generally based on general rules organising civil liability. See Section 4.3.3.2 of the current report relating to freedom of expression and the MANDOLA deliverable D2.1 - Definition of illegal hatred and implications, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, especially the Annex, http://mandola-project.eu/.

[121] Article 17 of the ECHR.

[122] See for example "The protection of health and morals" *in* Steven Greer, *The exceptions to Article 8 to 11 of the European Convention on Human Rights*, Human rights files n°15, Council of Europe publishing, 1997, p. 24, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf (last accessed on 12 May 2017).

[123] As mentioned above, a television presenter's capillary evolution has been considered as being a piece of information that anyone is legitimate to access. Moreover, the ECHR criteria in order to identify if a privacy limitation is legitimate, in case of publication of privacy information, is the contribution to a debate of "public

the ECHR in case of privacy limitation[124] might serve as a guide for behaviour. Indeed, these requirements aim at identifying the privacy limitations that will be considered as legitimate, *versus* the limitations that will be considered as privacy "violations"[125]. States have moreover the obligation to enforce the application of these requirements between individual themselves[126].

As a consequence, the sphere of protected privacy might more widely be identified as the whole sphere of information and freedoms that surround an individual, who will be identified as being their subject, and with which any interference of third parties must be legitimate, necessary and proportionate in the sense given to these terms by the ECHR and the ECtHR. In this sense, this sphere of protected privacy can only be assessed depending on the precise individuals who might interfere with this sphere, and, again, depending on the ways and morals that are admitted as being legitimate, necessary and proportionate at a given time.

4.1.2.5.3 No matter of whether a non-protected given element of life still belongs to privacy or not

The definition we propose covers the right to privacy as it seems to be protected by law, but does not take sides on whether it stays or not in the "privacy zone" in cases it is not any more protected, even temporarily. More precisely, when a person accesses a personal information related to another person or restrains the freedom of private life of this other person with the agreement of this latter person or on the basis of another legitimate justification, remains the question of whether the accessed element or the restricted freedom stays in the privacy zone, and is only less protected by law than the other elements of this zone in these particular circumstances[127], or if this accessed element or this restricted freedom leaves the privacy sphere under this meaning, at least temporarily and in respect of only certain third parties, and therefore does not belong anymore to the privacy sphere towards these latter third parties during the time of the absence or the reduction of its legal protection[128].

---

interest", which must be noticed, even where the disclosed privacy elements concern a public figure (1). The question of whether the capillary evolution of a television presenter is or not a contribution to a debate of public interest stays open. (1) See for example ECtHR, 3rd Sect., 24 June 2004, *von Hannover v. Germany*, appl. n°59350/00, §57, http://hudoc.echr.coe.int/eng?i=001-61853 (last accessed on 12 May 2017); Alexis Guedj, « La presse "people" face à la Cour européenne des droits de l'homme », Légipresse n° 217, Dec. 2004, chron., p. 137, referring to § 59 of the above-mentioned ECtHR court case; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 114.

[124] See below Section 4.1.3.

[125] This terminology can be found in all ECtHR decisions.

[126] See for example ECtHR, 3rd sect., *von Hannover v. Germany*, *op. cit.* §57.

[127] This leads systematically to a (legitimate) limitation of privacy, whether the concerned individual lives it as a positive or negative experience. This corresponds notably to the analysis of Ruth E Gavinson, in "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, particularly p. 428, available at http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (last accessed on 12 May 2017): "*A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him*".

[128] This implies that privacy, composed of the other remaining elements, is not considered as limited or restricted. In a close sense, see Edward Shils (quoted by Ruth E. Gavinson, *op. cit*., p. 428), who argues that any

A right to be forgotten does exist in both these analyses: the private element is protected again once third parties lose their legitimacy to restrict its exercise or to reduce the scope of its confidentiality, regardless of whether we consider that this element returns into the privacy sphere or that this element had remained into the privacy sphere and benefits again from the entire legal protection due in this respect.

This being said, the ECHR and the ECtHR distinguish between legitimate private life limitations and arbitrary private life limitations, which could be understood as implying that a private element which is temporarily unprotected or less protected for legitimate reasons remains a privacy component in nature. Moreover, the simple fact that a legal protection remains, which consists basically in verifying that the privacy limitation stays legitimate and does not become arbitrary, enables also considering that the personal element stays private in nature, and that its legal protection only differs -being limited to the verification of existing guarantees against arbitrariness-, to enable interactions with third parties.

In any case, even if our preference would be to consider, for the above-mentioned reasons, that a temporarily less protected privacy element stays private in nature, despite its casuistic lower protection, this theoretical debate does not need to be settled since it has no practical implications. Indeed, a less protected privacy element in certain circumstances might be highly protected in other circumstances, and must in this sense be considered as belonging to privacy as long as its limitation does not meet the conditions required by the EHR and the ECtHR.

In conclusion, the more relevant definition of privacy appears to be a negative definition in relation to third parties' rights, applied to the confidentiality and to the freedom of private life. However, this definition is not exempt from a dependency on ways and morals of the time, and must always be confronted to these values where the purpose is to identify precisely the elements that must be seen as belonging to the protected private sphere of a given individual.

More precisely, **the notion of private life or privacy can be understood as being composed of two groups of elements:**

- All the pieces of information related to personal life over which third parties have no legitimacy of control, control that may for instance consist of knowing, collecting, using, repeating or publishing the information;
- All the freedoms exercised in the personal sphere (in other words the freedom of privacy), with which third parties must not interfere, and which may themselves be the subject of personal information.

In this definition,

privacy limitation which is controlled by the individual does not constitute a loss of privacy : "*Privacy exists where the persons whose actions engender or become the objects of information retain possession of that information, and any flow outward of that in-formation from the persons to whom it refers (and who share it where more than one person is involved) occurs on the initiative of its possessors*". A similar theory is developed by Adam D Moore, *Privacy Rights: Moral and Legal Foundations*, Pennsylvania State University press, 2010: "Privacy may be understood as the right to control access to and use of physical items, like bodies and houses, and information, like medical and financial facts" (p. 5); Charles Fried, "*who understands privacy as control over information*": Daniel J. Solove, *Understanding privacy*, Harvard University Press, 2008, quotation p. 35.

- The notion of "personal information" refers to any information related to someone's life, that is to say to any "objective" information that can be associated with this person as a "subject"[129], this latter person being directly or indirectly identifiable;
- The notion of "third parties" refers to natural and legal persons, including States;
- The notion of "legitimacy" refers to the "right"[130] that entitle third parties to penetrate another person's personal sphere.
    - This right must be prescribed or at least authorised by law, and its exercise must be restricted to measures that are legitimate, necessary and proportionate[131]. Ways and morals of a time might have to be considered here, since they especially determine what it is common to do or to not do in certain circumstances, what it is admitted in terms of being at a certain place at a certain moment or of behaving in a certain manner in certain circumstances[132], or even determine what should or not contribute to a debate of public interest[133].
    - The boundaries of this right might alternatively be determined by the person whose private life is concerned, when law does not render such consent ineffective.

As a consequence, the sphere of protected privacy might more widely be identified as the whole sphere of information and freedoms that surround an individual, who will be identified as being their subject, and with which any interference of third parties must be legitimate, necessary and proportionate in the sense given to these terms by the ECHR and the ECtHR. In this sense, this sphere of protected privacy can only be assessed depending on the precise individuals who might interfere with this sphere, and, again, depending on the ways and morals that are admitted as being legitimate, necessary and proportionate at a given time.

[129] On this definition, see Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit*. n° 33 and s.

[130] Such a "right" to enter in the private zone of another individual is not necessarily a subjective right, in other words a right that is binding on third parties and whose respect or entitlement may be requested before a court. It may be only belong to the general "freedom" that exists in case there is no prohibition, and therefore be an admitted behaviour to the extent it is not faulty - in other words to the extent it is legitimate, necessary and proportionate (see Section 4.1.3). Such right may moreover be limited in time.

[131] See below Section 4.1.3.

[132] See for example "The protection of health and morals" *in* Steven Greer, *The exceptions to Article 8 to 11 of the European Convention on Human Rights*, Human rights files n°15, Council of Europe publishing, 1997, p. 24, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf (last accessed on 12 May 2017).

[133] See for example ECtHR, 3rd Sect., 24 June 2004, *von Hannover v. Germany*, appl. n°59350/00, §57, http://hudoc.echr.coe.int/eng?i=001-61853 (last accessed on 12 May 2017).

4.1.3 Nature and extent of the private life protection

Privacy protection is generally covered by civil law at national levels[134], in addition to administrative or public law where the State is involved. Some criminal provisions do exist, but they are only targeting some private life aspects, for example the secrecy of correspondence[135] and the secrecy of the voice and image of a person[136]. Criminal law will therefore not be included in our analysis.

Fort the rest, any limitation of the right of private life must comply with four general principles that we will analyse in details.

4.1.3.1 Any limitation must comply with four general principles

In the European Union, private life protection is ensured by the European Union Court of Justice (CJEU), on the basis of the European Union law[137], and by the ECtHR, on the basis of article 8 of the eponymous Convention[138]. That is to say that both courts refer - at least - to the ECHR principles, since privacy is mainly protected in the EU by the EUCFR[139], which, as mentioned in the introduction of the current study, has the same meaning and scope as the ECHR as regards the so-called "*conditional*" right[140] to private life, even though European Union law may provide more extensive protection. National Courts also refer to the ECtHR protection requirements since, as seen previously in our Section 3.2, the ECtHR applies in all the EU Member States.

---

[134] For example, article 9 of the French civil Code; art. 74 of the new Romanian civil Code.

[135] For example, Article 226-15 of the French penal Code holds: "*Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of €45,000*"; "*The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions*". 432-9 of the French penal Code holds: "*Except where provided for by law, the ordering, committing or facilitation of the misappropriation, suppression or opening of correspondence, and the disclosure of the contents of such correspondence, by a person holding public authority or discharging a public service mission acting in the course of or on the occasion of his office or duty, is punished by three years' imprisonment and a fine of €45,000*"; "*The same penalties apply to the persons referred to under the previous paragraph, or to employees of electronic communication networks open to the public, or to employees of a supplier of telecommunication services, who, acting in the performing of their office, order, commit or facilitate, except where provided for by law, any interception or misappropriation of correspondence sent, transmitted or received by a means of telecommunication, or the use or the disclosure of its contents*";.

[136] For example, article 226-1 of the French penal Code; art. 226 of the new Romanian criminal Code.

[137] See the Court of Justice of the European Union's website, at http://curia.europa.eu/jcms/jcms/Jo2_7024/ (last accessed on 12 May 2017).

[138] Even if the competences of the ECtHR are going beyond the European Union, since 47 countries have signed or accessed to the European Convention on Human RIghts.

[139] The more specific issue of personal data protection will be dealt with in the following sections.

[140] Some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression (see for ex. Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pages 44-45).

The conditions under which a limitation of the right to private life is possible, according to Article 8, 2 of the ECHR as interpreted by the ECtHR, and which are to be interpreted narrowly[141], are the following: the **limitation must have a specific, clear, accessible and foreseeable legal basis, must be in conformity with one of the legitimate aims** listed in the Convention and must **be "*necessary* *in a democratic society for the aforesaid aim*"**[142], which implies that the interference, "*in a society that means to remain democratic*"[143], must correspond to a "*pressing social need*"[144], and must **be "*proportionate* *to the legitimate aim pursued*"**[145].[146] Certain legal authors refer to these requirements as a "*general public order clause*"[147].

> The ECtHR notably pointed out that systems of secret surveillance must contain safeguards established by law, which apply to the supervision of the relevant services' activities[148]. It recalled "*the danger (a law establishing secret surveillance) poses of undermining or even destroying democracy on the ground of defending it*", affirming that "*the Contracting States may not, in the name of the struggle against espionage and*

[141] See for instance ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §38, http://hudoc.echr.coe.int/eng?i=001-57805 (last accessed on 12 May 2017).

[142] See for instance ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 45, Series A, n° 30, http://hudoc.echr.coe.int/eng?i=001-57584 (last accessed on 12 May 2017).

[143] Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, §8, available under the Sunday Times court case, *op cit*.

[144] ECtHR, *Sunday Times v. The United Kingdom, op cit*, § 59.

[145] ECtHR, *Sunday Times v. The United Kingdom, op cit,* § 63. See also Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, under the dir. of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p. 43; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 86.

[146] On this discussion see Estelle De Marco *in* C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking – balancing cybercrime responses in democratic societies*, oct. 2009, p. 207, http://www.aconite.com/blocking/study. The French translation of this study, by Estelle De Marco and Frédéric Nguyen, May 2017, is available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique/ (last accessed on 12 May 2017); see also Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 *et seq*., especially p. 24.

[147] Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", *op.cit.*, pages 44-45.

[148] See for instance ECtHR, 3rd Sect., 29 June 2006, *Weber and Saravia v. Germany*, n° 54934/00, §94, http://hudoc.echr.coe.int/eng?i=001-76586; European Court of Human Rights, *Internet: case-law of the European Court of Human Rights*, June 2015, p. 10, http://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis and more precisely at http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (URLs last accessed on 2 May 2017).

terrorism, adopt whatever measures they deem appropriate"[149]. This statement was recalled by the Article 29 Data Protection Working Party[150].

The previous four principles (legal basis, legitimate aim, necessity and proportionality to the aim pursued of a privacy restrictive measure, in order to see it as legitimate and not as privacy "violation"[151]) constitute general principles of the Union's law[152]. They are therefore very often recalled in the European legal instruments, and, sometime with a few variations, are reflected in national laws, in addition to influencing national constitutional courts such as the French Constitutional Council[153] and the Romanian Constitutional Court[154].

Since the Treaty of Lisbon came into force, these four principles are also fully integrated within the European Union law. Indeed, Article 52, 1 of the EU Charter of Fundamental Rights recalls that any limitation of the rights and freedoms it recognises "*must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".

We can notice that, in this wording, the principle of necessity may be understood as being included in the principle of proportionality[155]. In the same line, Advocate General Poiares Maduro considers that "*the concept of necessity [...] is well established as part of the proportionality test*"[156]. Conversely, the CJEU seems sometime to include the principle of

[149] ECtHR, plen., 6 September 1978, *Klass and others v. Germany*, appl. n°5029/71, §49, http://hudoc.echr.coe.int/eng?i=001-57510 (last accessed on 12 May 2017).

[150] Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, adopted on 9 November 2004 (WP 99), page 4.

[151] ECtHR, *Sunday Times v. The United Kingdom, op cit*, § 45.

[152] Article 6, 3 of the Treaty on European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:C2010/083/01&from=FR.

[153] The French Constitutional Council recognises the exclusive competence of the Parliament to hold limitations to freedoms, accordingly to article 34 of the Constitution and art. 4 of the French Human and Citizen Rights Declaration of 1789. This Council also considers that the lawmaker "*can only limit the exercise of a freedom for a constitutional imperative*" (see Frédérique Lafay, note under the Council decision of 18 January 1995, JCP 95, II, 22 525). This council considers furthermore that "*any restrictions placed on the exercising of (freedoms) must necessarily be adapted and proportionate to the purpose it is sought to achieve"* (see for instance Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 15).

[154] See for instance the Decision n° 1258/2009, available in English language at http://www.legi-internet.ro/en/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html (last accessed on 12 May 2017).

[155] In this sense, see for example C-92/09 Volker und Markus Schecke GbR v. Land Hessen, and C-93/09, Eifert v. Land Hessen and Bundesanstalt fur Landwirtschaft und Ernahrung, 9.11.2010. A summary is available in Laraine Laudati (OLAF DPO), EU court decisions relating to data protection, December 2012, p. 11, available at http://ec.europa.eu/anti_fraud/documents/data-protection/dpo/ecj_decisions_relating_data_protection_en.pdf (last accessed on 12 May 2017).

[156] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 5.7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

proportionality in the meaning of the term "necessary". For example, the Court states: "*in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Art.s 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question*"[157].

However, discordances of classification are common, since the principles of necessity and of proportionality are both contained in the ECHR formula: "*necessary in a democratic society*", and therefore are both covered by the term "necessary"[158], even if the most cited and perhaps most important principle is proportionality[159]. What is important to notice is that both Courts and all the legal analysts of their court cases recognise that necessity and proportionality imply a certain number of obligations, which are the ones we will analyse below, whatever they are classified as obligations ensuring necessity or obligations ensuring proportionality. In that line, the Article 29 Data Protection Working Party[160] has emphasised that the Court of Justice of the European Union (CJEU) has an approach which is "*largely consistent*" with the E. Court H. R.'s one[161], and has made recent efforts to apply the principles of necessity and proportionality, as they were developed by the ECtHR, to article 7 and 8 of the EUCFR[162].

Before analysing in details these four principles, it should be noted that, according to the CJEU (which follows the ECtHR's approach), any measure that derogates from the system of protection of the right to privacy is an interference, "*no matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way*"[163].

4.1.3.2 Details of requirements

Privacy limitations must have a specific, clear, accessible and foreseeable legal basis, must be in conformity with one of the legitimate aims listed in the Convention, must be necessary and must be proportionate.

---

[157] CJEU, *Schwarz v. Stadt Bochum*, C-291/12, 17 October 2013, §46, quoted by the Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.31.

[158] See for example ECtHR, 5th Sect., 19 May 2016, *DL v. Bulgaria*, appl. n° 7472/14, §105, http://hudoc.echr.coe.int/eng?i=001-163222 (last accessed on 12 May 2017).

[159] See *infra*.

[160] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.30.

[161] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 4.2.

[162] For an example of such application, see CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 12 May 2017).

[163] CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, *op. cit*., §33.

1. A specific, clear, accessible, stable and foreseeable legal basis

Any interference with the right to private life must be lawful, that is to say it must be "*prescribed by law*" according to the ECtHR, expression that must be understood as pursuing the same aim as the expressions "*in accordance with the law*"[164], "*in accordance with law*", or "*provided for by law*", within the convention and its protocols[165]. Indeed, all these expressions, which are "*equally authentic but not exactly the same*", are translated by the French expression "*prévues par la loi*", and the ECtHR must "*interpret them in a way that reconciles them as far as possible and is most appropriate in order to realise the aim and achieve the object of the treaty*"[166].

These expressions mean firstly "*that any interference must have some basis in the law of the country concerned. However, over and above compliance with domestic law, it also requires that domestic law itself be compatible with the rule of law. It thus implies that there must be a measure of legal protection in domestic law*", including "*against arbitrary interferences by public authorities" with the right to private life*[167].

As regards the quality of the law, the ECtHR developed three main requirements which all contribute to a fourth one which is the requirement of predictability: the law that organises the limitation of the right to privacy must be sufficiently clear and precise. It must be accessible, and it must be stable.

1.1 Clear and precise

Law must notably be "*formulated with sufficient precision to enable the citizen to regulate his conduct*: *he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*"[168].

In the special context of interception of communications for the purposes of police investigations, the ECtHR considers that "the *requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same (…) as they are where the object*

---

[164] This is the terminology used by the ECHR. The EUCFR mentions "*provided for by law*": Article 52.1.

[165] See ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 48, http://hudoc.echr.coe.int/eng?i=001-57584 (last accessed on 12 May 2017).

[166] See ECtHR, *Sunday Times v. The United Kingdom*, *op. cit*. § 48.

[167] ECtHR, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19, http://www.cnpd.public.lu/fr/legislation/jurisprudence/cedh/cedh_caselaw_dp_fr.pdf, referring to ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §§66 *et seq*., http://hudoc.echr.coe.int/eng?i=001-57533 (Violation of Article 8 of the Convention - Interception of postal and telephone communications and release of information obtained from "metering" of telephones, both effected by or on behalf of the police within the general context of criminal investigation) (URLs last accessed on 12 May 2017).

[168] All quotations are coming from the European Court of Human Rights case *Sunday Times v. The United Kingdom*, *op cit*, § 49. See also Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, page 43; Steve Foster, *Human Rights and Civil Liberties*, 2nd ed., 2008, p. 464.

of the relevant law is to place restrictions on the conduct of individuals"[169]. As a consequence, in particular, the law does not have to be such *"that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly"*[170]

However, in this context, the principle of clarity implies that the law, in order "*to be compatible with the rule of law*"[171], is "*sufficiently clear in its terms to give citizens an* ***adequate indication as to the circumstances in which and the conditions on which public authorities are empowered*** *to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*"[172]. Law must further "***indicate the scope (...) and the manner of (...) exercise****"*[173] of the power conferred to competent authorities, "*with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*"[174].

The clear and precise definition [175] of the scope and the manner of exercise of the power which limits fundamental rights, which is for example also required by the French constitutional Council[176], implies firstly to exclude any "obscurity and uncertainty as to the state of the law"[177]. Secondly, it implies that « *there exist adequate and effective guarantees against abuse*"[178].

---

[169] ECtHR, *Malone v. The United Kingdom*, §67, *op. cit*.; Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), *op. cit*., p. 19; In the same line see ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, http://hudoc.echr.coe.int/eng?i=001-60696 (last accessed on 12 May 2017), related to covert surveillance by public authorities.

[170] *Ibid.*

[171] ECtHR, 3rd Sect., 12 May 2000, *Khan v. The United Kingdom*, appl. n° 35394/97, §26, http://hudoc.echr.coe.int/eng?i=001-58841 (last accessed on 18 May 2017).

[172] ECtHR, *Malone v. The United Kingdom*, §67, *op. cit*.; See also all the references in footnote n°147.

[173] ECtHR, *Malone v. The United Kingdom*, §68*, op. cit*.; ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, §65, http://hudoc.echr.coe.int/eng?i=001-160020 (last accessed on 18 May 2017); Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), *op. cit*., p. 19.

[174] *Ibid.*

[175] ECtHR, ch., 24 April 1990, *Huvig v. France*, appl. no 11105/84, §32 ("*clear, detailed rules*"), http://hudoc.echr.coe.int/eng?i=001-57627 (last accessed on 18 May 2017).

[176] The French Constitutional Council considers more globally that the principles of clarity, accessibility and intelligibility of the law impose on the law-maker to "adopt disposals of sufficient precision and non-equivocal formula in order to prevent subjects of the law from an interpretation that would be in opposition with the Constitution or from the risk of arbitrary": French Constitutional Court, decision n° 2004-503 of 12 August 2004, § 29, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-503-dc/decision-n-2004-503-dc-du-12-aout-2004.908.html (last accessed on 12 May 2017).

[177] . ECtHR, *Malone v. United kingdom,* §79*, op. cit.*; French Constitutional Council, Decision n° 2004-503 DC of 12 August 2004, *op.cit.,* § 29.

[178] ECtHR, plen., 6 September 1978, *Klass and other v. Germany*, appl. n°5029/71, §50, http://hudoc.echr.coe.int/eng?i=001-57510 (last accessed on 18 May 2017) ; French Constitutional Council, Decision n° 2013-357 QPC of 29 November 2013, *Société Wesgate Charters Ltd*, cons. 8, http://www.conseil-

This principle, applicable in the area of communications intercept performed by the judicial authority[179] and by intelligence services[180], is a legal certainty requirement[181] and can be transposed to data capture more generally since it concerns any storage of private information by public authorities[182], in particular within the context of "*the development of surveillance methods resulting in masses of data collected*"[183] (which must be accompanied by a "*simultaneous development of legal safeguards securing respect for citizens' Convention rights*"[184]).

1.2 Adequately accessible

Domestic law must also "*be adequately accessible*", meaning that "*the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case*"[185]. This implies firstly that the legal basis is easily accessible to concerned citizens[186]. This implies secondly that the provisions which authorise the limitation of freedom is intelligible "*in the light of the legal corpus in which they are intended to be part of*" [187]. Therefore the whole of this corpus must be consistent[188], in order to fully meet the requirement of predictability[189]. In other words, the

constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2013/2013-357-qpc/decision-n-2013-357-qpc-du-29-novembre-2013.138841.html (last accessed on 18 May 2017).

[179] ECtHR, *Khan v. United kingdom*, §22s, *op. cit.*

[180] See for ex. ECtHR, *Malone v. United kingdom,* §67*, op. cit.*

[181] ECtHR, 28 March 2000, ch., *Baranowski v. Poland*, appl. n°28358/95, §52, http://hudoc.echr.coe.int/eng?i=001-58525 (last accessed on 18 May 2017); French Conseil d'État, « Sécurité juridique et complexité du droit » in *Rapport public 2006 - Sécurité juridique et complexité du droit*, éd. du Conseil d'État, coll. « Études et documents du Conseil d'État », p. 281, http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Securite-juridique-et-complexite-du-droit-Rapport-public-2006 (last accessed on 18 May 2017); The condition of clarity of the law was also linked to the legal security principle by the Court of Justice of the European Union: see Frédéric Pollaud-Dulian, "A propos de la sécurité juridique", RTDCiv. (3) juill.-sept. 2001, p. 487, ref. p. 489.

[182] ECtHR, gr.ch., 4 May 2000, *Rotaru v. Romania*, appl. n°28341/95, §45 *et seq,* http://hudoc.echr.coe.int/eng?i=001-58586 (URLs last accessed on 12 May 2017).

[183] ECtHR, *Szabó and Vissy v. Hungary, op. cit.* §68.

[184] *Ibid.*

[185] ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 49, http://hudoc.echr.coe.int/eng?i=001-57584 (last accessed on 12 May 2017). On this question, see also Pascale Deumier, « La publication de la loi et le mythe de sa connaissance », Les petites affiches, 6th March 2000, n° 46.

[186] Ex. ECtHR, ch., 24 April 1990, *Huvig v. France*, appl. n° 11105/84, §33, http://hudoc.echr.coe.int/eng?i=001-57627 (last accessed on 18 May 2017).

[187] Translated from French. French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit*., p. 282.

[188] *Idem*, pp. 282 et 288. Principles of consistency and intelligibility of legal texts as a whole are most of the time implicit in the ECtHR jurisprudence (see for ex. ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §66, http://hudoc.echr.coe.int/eng?i=001-57533). However see ECtHR, ch., 16 December 1992, *de Geouffre de la Pradelle v. France*, appl. n°12964/87, §34, http://hudoc.echr.coe.int/eng?i=001-57778; ECtHR, gr.ch., 15 October 2015, *Perinçek v. Switzerland*, appl. n° 27510/08, §134, http://hudoc.echr.coe.int/eng?i=001-158235 (URLs last accessed on 18 May 2017).

[189] ECtHR, *Huvig v. France*, *op. cit.* §26.

"*physical*" [190] access to the legal basis must be accompanied by an "*intellectual*" [191] access to this legal basis.

This being said, the term "Law" is understood by the ECtHR "*in its substantive sense, not its formal one*". In consequence, it does not only refer to legislative texts, but it also includes *"non-written law*", "*enactments of lower rank than statutes*", and case law. "*In a sphere covered by the written law, the "law"*" is therefore "*the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments*"[192].

1.3 Stable

A law that can "*reasonably*"[193] be foreseen must be stable[194], this principle being also linked to the requirement of legal certainty[195]. In addition, the principle of stability favours the general public's confidence in the legal system, such confidence being "*one of the essential components of a State based on the rule of law*" [196]. The principle of stability especially means no unpredictable variations[197] and, potentially, no too frequent variations[198].

---

[190] Translated from French. Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (n°29), p.4, https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm (last accessed on 18 May 2017).

[191] *Idem.*

[192] All quotations are coming from ECtHR, ch., 24 April 1990, *Kruslin v. France*, appl. n°11801/85, §29, http://hudoc.echr.coe.int/eng?i=001-57626. On this issue see also Frédéric Sudre, op cit, page 43; R. Koering-Joulin, D. 90, chron. p. 187. See Estelle De Marco *in* C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, p 182, available at http://www.aconite.com/blocking/study; French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ (URLs last accessed on 12 May 2017).

[193] See for ex. ECtHR, gr. ch., 15 October 2015, *Perinçek v. Switzerland*, appl. n°27510/08, §134, http://hudoc.echr.coe.int/eng?i=001-158235 (last accessed on 18 May 2017).

[194] See for ex. ECtHR, 1st sect., 30 July 2015 (final: 30/10/2015), *Ferreira Santos Pardal v. Portugal*, appl. n°30123/10, §42, f, http://hudoc.echr.coe.int/eng?i=001-156500 (URL last accessed on 19 May 2017).

[195] *Idem* ; French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.*, p. 281.

[196] See for ex. ECtHR, 3rd Sect., 1st December 2005, *Păduraru v. Romania*, appl. n°63252/00, §98, http://hudoc.echr.coe.int/eng?i=001-71444 (last accessed on 19 May 2017); ECtHR, *Ferreira Santos Pardal v. Portugal, op. cit.* §42, f.

[197] ECtHR, 30 July 2015, *Ferreira Santos Pardal v. Portugal*, *op. cit.* §43-49; French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281.

[198] French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281. See ECtHR, ch., 16 December 1992, *de Geouffre de la Pradelle v. France*, appl. n°12964/87, §33, http://hudoc.echr.coe.int/eng?i=001-57778; Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (n°29), pp. 13 and seq., https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm; Dominique J. M. SOÛLAS de RUSSEL, Philippe RAIMBAULT, « Nature et racines du principe de sécurité juridique : une mise au point », RIDC, 2003, vol. 55, n°1, p. 90, referring to ECtHR, plen., 13 June 1979, *Marckx v. Belgium*, appl. n°6833/74, http://hudoc.echr.coe.int/eng?i=001-57534 (URLs last accessed on 18 May 2017).

2. A legitimate aim

Article 8, 2 of the ECHR lists exhaustively the legitimate aims for which an interference with the right to privacy may be legitimate. These aims are the interests of national security, public safety or the economic well-being of the country; the prevention of disorder or crime; the protection of health or morals, and the protection of the rights and freedoms of others.

This notion of legitimate aim is also considered by the Court of Justice of the European Union[199]. In addition, the EUCFR requires that private life limitations must "*genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*"[200].

3. The necessity of the interference

This principle of "necessity" of the interference consists in the **demonstration that this interference is actually appropriate to satisfy a specific societal need**.

Indeed, according to the ECtHR, any limitation of private life, in order to be legitimate, must be a need, and this need must be established convincingly[201]. The latter term "need" refers to two different kind of needs: a "pressing social need" (i.e. a societal issue that needs to be addressed[202]), and a need for the specific proposed interference (which must be appropriate to satisfy the identified social need[203]).

Therefore, the principle of necessity is divided in two requirements:

3.1 The demonstration of a specific societal need

The interference must be "*necessary having regard to the facts and circumstances prevailing in the specific case*"[204], which implies firstly **identifying "*the specific societal***

[199] See for example CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §46, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 12 May 2017).

[200] Article 52.1 of the Charter.

[201] ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §38, http://hudoc.echr.coe.int/eng?i=001-57805 (last accessed on 12 May 2017): "*the need for an interference* (...) *in a given case must be convincingly established*". In the same spirit, see the Opinion of the European Data Protection Supervisor, on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 26 September 2005, § 10, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_EN.pdf (last accessed on 12 May 2017).

[202] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.13, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[203] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.17, 3.19.

[204] ECtHR, *Sunday Times v. The United Kingdom*, *op. cit*, § 65.

need to be addressed", "*within the broader sphere of the legitimate aim pursued",* with a view to protecting this particular aim[205].

This need must be "pressing", in other words it must have a certain "***level of severity, urgency or immediacy***"[206]. Harm may result on society if the need is not addressed, taking into account the views of society and potentially divergent opinions regarding this particular "need"[207].

Moreover, the existence of this severe or urgent need **has to be proven**. For instance, in a case where the applicant had been prevented to make certain statements relating to the dangers of microwave ovens, the ECtHR concluded that "*there was no evidence that the sale of microwave ovens had been affected by the applicant's remarks*".[208]

3.2 The demonstration that the interference is suited to satisfy that need

Establishing the need for interference, in a given case, also means establishing that this interference is appropriate to reach the aim pursued, in other words that it effectively may mitigate the harm caused to society[209].

For instance, the European Data Protection Supervisor recalled that "*statements of Member States on whether they consider data retention a necessary tool for law enforcement purposes*" do not "*as such establish the need for data retention as a law enforcement measure*", and that "*the statements on the necessity should be supported by sufficient evidence*"[210].

In the same line, the Article 29 Data Protection Working Party noticed, in 2004, that the framework decision on data retention which proposed a "*comprehensive storage*

---

[205] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.13.

[206] Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), *op. cit*., 3.14.

[207] Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), *op. cit*., 3.17 - 3.19.

[208] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 *et se*q., quotation p. 25, in relation with ECtHR, ch., 25 August 1998, *Hertel v. Switzerland*, appl. n° 25181/94, http://hudoc.echr.coe.int/eng?i=001-59366 (last accessed on 12 May 2017). Jeremy McBride considers this requirement (consisting in determining "*whether there was a sufficient basis for believing that a particular interest was in peril*") as being a "proportionality" requirement. However, together with the Article 29 Data Protection Working Party (see footnotes above), we rather believe that this requirement is a condition of the "necessity" of an interference, not a condition of its proportionality. However, this discordance of opinions has no practical impact, since it is in any cases a requirement which will base the assessment of the Court.

[209] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.19. In the same sense see also CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §49, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 12 May 2017), which verifies whether the interference "*is appropriate for attaining the objective pursued*".

[210] Opinion of the European Data Protection Supervisor, on the Evaluation report from the Commission to the Council and the European Parilament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, § 41, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf (last accessed on 12 May 2017).

of all traffic data, user and participant data", did not provide "*any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security*". The Working Party also noticed that "*representatives of the law enforcement community have failed to provide any evidence as to the need for such far reaching measures*"[211].

More recently, the CJEU recalled that "*the principle of proportionality*[212] *requires that acts of the EU institutions* ***be appropriate for attaining the legitimate objectives pursued*** *by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*"[213]. However, unlike the two authorities quoted above, the EUCJ considered that the retention of traffic data "*may be considered to be appropriate for attaining the objective pursued*" by the Data Retention Directive[214]. The EUCJ challenged the validity of the Data Retention Directive in the light of Article 7 of the EUCFR, not on the basis of the principle of necessity, but on the basis of the principle of proportionality that we will analyse later in this study, the interference being not limited to what is strictly necessary to achieve its objectives.

Before analysing this principle of proportionality, it is worth noticing that the research of the necessity of an interference may imply reviewing "*the effectiveness of existing measures*" aiming at addressing the targeted pressing social need, "*over and above the proposed measure*", and explaining "*why these existing measures are no longer sufficient*" and how the proposed measure will bring remedies[215].

4. The proportionality of the limitation to the aim pursued

The principle of proportionality[216] is "*recognised as one of the central principles governing the application of the rights and freedoms*" contained in the ECHR and its additional

---

[211] Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", adopted on 9 November 2004, WP99, quotations page 4, available at the following address: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf (last accessed on 12 May 2017).

[212] This principle includes, in this formula, the principle of necessity (Advocate General Poiares Maduro for instance considers that *"the concept of necessity [...] is well established as part of the proportionality test*" (Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 5.7). For further analysis of discordances of classification, see the introduction of our Section 4.1.3.

[213] CJEU, *Digital Rights Ireland and Seitlinger e.a*., joint cases C-293/12 and C-594/12, 8 April 2014, §46, available at http://curia.europa.eu/juris/liste.jsf?language=fr&td=ALL&num=C-293/12 (last accessed on 12 May 2017).

[214] CJEU, *Digital Rights Ireland and Seitlinger e.a*., joint cases C-293/12 and C-594/12, 8 April 2014, *op. cit*., §49.

[215] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[216] On the entire subsection see Estelle De Marco *in* C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*", October 2009, Section 7.5.2, http://www.aconite.com/blocking/study; French version available at

Protocols.[217] Allowing "*some evaluation of how much of a contribution a particular restriction can make towards securing a given objective*",[218] the principle of proportionality satisfies "*the need for balancing entailed when giving effect to the rights*" that are concerned by the ECHR requirements. Indeed, without this requirement, "*the formulation of Convention provisions would be open to restrictions depriving the rights and freedoms of all content so long as they were prescribed by law and for a legitimate purpose*"[219], in addition to answering a pressing social need.

In the light of the ECtHR court cases, the proportionality of a measure that limits freedoms implies that this measure or interference does not go "*further than needed to fulfil the legitimate aim being pursued*"[220], and is surrounded by appropriate safeguards.

4.1 The interference must be strictly necessary[221]

The limitation of a conditional fundamental right must be strictly necessary to the aim pursued, and, in relation with the monitoring of communications by public authorities, must be "*strictly necessary, as a general consideration, for the safeguarding of the democratic institutions and, moreover, (...) strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation*"[222].

This principle implies an effective assessment of the strict necessity of the measure in relation with its:

- context[223]: adapting the interference to its context means inter alia taking into account several elements such as the severity of the social need and the "*proportionality of the very behaviour which is being restricted*"[224].
  - The severity of the social need:

    Depending on the seriousness of the issue to be addressed, whatever measures will not be considered as appropriate. As it has been

http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ (URLs last accessed on 12 May 2017).

[217] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 *et seq*., quotation p. 23.

[218] Jeremy McBride, *op cit, p. 24*.

[219] Jeremy McBride, *op cit,* p. 24.

[220] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.20.

[221] For an application of this principle by the CJEU, see for example CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §§ 46, 56 and 65, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 12 May 2017).

[222] ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, §73, http://hudoc.echr.coe.int/eng?i=001-160020 (last accessed on 18 May 2017).

[223] See for ex. ECtHR, ch., 24 February 1997, *De Haes et Gijsels v. Belgium,* appl. n°19983/92, http://hudoc.echr.coe.int/eng?i=001-58015 (last accessed on 18 May 2017).

[224] Jeremy McBride, *op cit*, pp. 25.

highlighted by the Article 29 Data Protection Working Party"[225], "*the more severe the issue and/or the greater or more severe or substantial the harm or detriment which society may be exposed to, the more an interference may be justified".* When the aim of the interference is public security, and more specifically prevention and detection of crime, the severity of the social need must be assessed having regards to the specific crime the measure is intended to address[226], and to the harm that crime would cause to society if not addressed.

- The proportionality of the restricted behaviour:

  Whatever the severity of the societal issue to be addressed, the proposed measure may cause harm to individuals to a lesser or greater extent, and the more this extent is, the less the interference is appropriate[227]. The "*nature of the activity being affected*" (sensitivity, high expectation of privacy…)[228] needs therefore to be taken into account. For example, "*the privacy considerations in terms of context are very different when installing CCTV cameras on a public street as opposed to installing them in toilets or hospital wards*"[229]. In the same spirit in relation to freedom of expression, the ECtHR considered that the "*remarks made by journalists about the conduct of views of judges and politicians*" were appropriate and could not be punished, considering " *they had sufficient factual basis to fall within the protection extended to the expression of value judgments under Article 10"*[230].

  The proportionality of the very behaviour that is being restricted may also depend on the characteristics of the individuals whose rights are

[225] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[226] The ECtHR noted for instance in a court case the lack of consideration of "*the nature or gravity of the offence*": Article 29 Data protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), op. cit., 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051 (last accessed on 12 May 2017).

[227] The Article 29 Data Protection Working Party covers this issue under the formula "*nature of the interference*": Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26.

[228] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211*), op. cit*., 3.26.

[229] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26.

[230] Jeremy McBride, *op. cit.*, pp. 25 and 26, referring to ECtHR, ch., 24 February 1997, *De Haes and Gijsels v. Belgium*, appl. n° 19983/92, http://hudoc.echr.coe.int/eng?i=001-58015, and ECtHR, ch., 1 July 1997, *Oberschlick v. Austria* (n°2), appl. n° 20834/92, http://hudoc.echr.coe.int/eng?i=001-58044 (URLs last accessed on 30 May 2017).

limited. Such a characteristic may be the age (for example, the age "*of the suspected offender*" when the aim of the interference is public security[231]), and the capacity of a given individual to adapt his or her behaviour to a given context[232].

- scope[233]: the scope of the interference must not exceed what is necessary to reach the aim pursued[234]. This means, *inter alia*, to limit to the greatest extent the volume of the intrusions into privacy (and, for example, of collected personal information), the number of places and people affected[235], the cases of exercise of the measure (LEAs' powers of decision and action must notably be limited to what is necessary), and the time during which the measure will be effective[236]. In addition, the "*overall effect*" of the interference must not lead to "*actually extinguish*"[237] a protected right:[238] (for instance, it "*was found to be unacceptable*" to prevent a person making statements in a situation where such a measure effectively prevented this individual "*making his contribution to the public debate*": this was affecting "*the very substance of his view*"[239]).

[231] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.,* 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051 (last accessed on 12 May 2017).

[232] In relation to an obligation to secure one's computer in order to prevent counterfeiting (knowing that computer security can never be ensured for sure), see Estelle De Marco, *Analyse du nouveau mécanisme de prevention de la contrefaçon à la lumière des droits et libertés fondamentaux*, 4 June 2009, Juriscom.net, http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/ (last accessed on 12 May 2017).

[233] See for ex. ECtHR, 5e sect., 19 May 2016, *D.L. v. Bulgaria*, appl. no7472/14, §105, http://hudoc.echr.coe.int/eng?i=001-163222 (last accessed on 19 May 2017).

[234] See for example ECtHR, 5th Sect., 19 May 2016, *DL v. Bulgaria*, appl. n° 7472/14, §105, http://hudoc.echr.coe.int/eng?i=001-163222 (last accessed on 12 May 2017). See also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26.

[235] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. no37138/14, *op.cit.* §§73 and 75-77. On this issue and the previous one see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26.

[236] On this issue and the previous one see for example ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §40, http://hudoc.echr.coe.int/eng?i=001-57805 (last accessed on 12 May 2017):

[237] Jeremy McBride, op cit, p. 24.

[238] In the same line, the CJEU verifies whether the interference may "*adversely affect the essence of the fundamental right*": CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §40, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 12 May 2017).

[239] Jeremy McBride, op cit, p. 25, referring to the court case Hertel v. Switzerland, judgment of the Court, 25 August 1998.

- nature[240]: the ECtHR also verifies if the interference's aim "*can be satisfactorily addressed in some other, less restrictive way*"[241]. For instance, "*an order requiring a journalist to disclose his source for a leak about the financial affairs of a company was considered to be unjustified (…) insofar as the objective was to prevent dissemination of confidential information since this legitimate concern was already being secured by an injunction restraining publication of the information that had been disclosed*"[242]. Therefore, "*an explanation of what other measures were considered and whether or not these were found to be more or less privacy intrusive should be presented. If any were rejected which were found to be less privacy intrusive, then the strong justifying reasons as to why this measure was not the one that was selected to be implemented should be given*"[243].

4.2 The interference must be limited by appropriate safeguards

Appropriate safeguards, in other words "*adequate and effective*"[244] safeguards, must firstly be implemented in order to palliate potential weaknesses of the necessity and proportionality tests[245], and in other words in order to limit the interference, in particular where technology used does not itself enable to limit the scope and the extent of the interference. These safeguards must secondly be implemented in order to "*render possible*"[246] the actual respect of these palliatives or limitations.

These safeguards, which must be clearly detailed in the legal basis[247], might especially be of an organisational[248] or of a technical[249] nature.

---

[240] See for ex. ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. n°17488/90, §42, http://hudoc.echr.coe.int/eng?i=001-57974 (URL last accessed on 18 May 2017).

[241] Jeremy McBride, op cit, p. 26. For an application of this principle at the EU level see for example a judgment of the European Union civil service tribunal (first chamber), *V. v. European Parliament*, 5 July 2011, case F-46/09, § 139, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=F-46/09 (last accessed on 12 May 2017).

[242] Jeremy McBride, op cit, p. 26, referring to ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. n°17488/90, http://hudoc.echr.coe.int/eng?i=001-57974 (last accessed on 18 May 2017).

[243] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 3.26, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[244] ECtHR, *Klass and others v. Germany*, *op. cit.* §§50s.

[245] ECtHR, plen., 6 September 1978, *Klass and others v. Germany*, appl. n°5029/71, §55, http://hudoc.echr.coe.int/eng?i=001-57510 (last accessed on 12 May 2017), referring to "*adequate and equivalent guarantees*" to be implemented in order to palliate the absence of effective remedy.

[246] Ex. ECtHR, plen., 13 June 1979, *Marckx v. Belgium*, appl. n°6833/74, §31, http://hudoc.echr.coe.int/eng?i=001-57534 (URLs last accessed on 18 May 2017).

[247] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., §§ 50-58, 59; see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26. See *supra*, in the bullet point dedicated to the legal basis of the interference.

Inter alia, where the interference is taken in the aim of ensuring public security, safeguards should include an indication of the "*grounds required for ordering*" the measures that constitute the interference[250], the cases in which the measure can take place[251], the length of the measure[252], the extent of LEAs' powers[253], and the way the respect of these restrictions will be enforced and controlled.

Control measures include the authorisation and/or supervision of an independent authority[254], which will ensure that the legal conditions for the interference are respected and will prevent any freedom of interpretation in relation to general terms potentially provided for by law. In principle, such independent control should be made by the judicial authority before the measure takes place, and a supervision of another nature is only permitted if the authority in charge of it provides the same guarantee of independence and expertise[255], posterior supervision being not permitted in all matters[256] since confidentiality cannot be restored once destroyed[257]. In addition, a judge from the judiciary should be involved "*at least in the last resort*"[258] in fields "*where abuse is potentially so easy in individual cases and would have (…) harmful consequences for democratic society as a whole*"[259], which is generally the case when the interference is organised for police purposes.

---

[248] See for ex. Article 29 Data Protection Working Party, Opinion 01/2014, *op. cit.*, 3.26; ECtHR, 4th Sect., 18 May 2010 (final 18 August 2010), *Kennedy v. The United Kingdom,* appl. n°26839/05, http://hudoc.echr.coe.int/eng?i=001-98473; ECtHR, 2nd Sect., 24 September 2002 (final 24 December 2002), *M.G. v. The United Kingdom*, appl. n°39393/98, http://hudoc.echr.coe.int/eng?i=001-60642; ECtHR, *Klass and others v. Germany*, *op. cit.* §. 56 (URLs last accessed on 18 May 2017).

[249] ECtHR, 18 May 2010, *Kennedy v. The United Kingdom*, *op. cit.*; ECtHR, 4th sect., 27 October 2015, *R.E. v. The United Kingdom*, appl. n° 62498/11, http://hudoc.echr.coe.int/eng?i=001-158159; ECtHR, gr.ch., 4 December 2015, *Roman Zakharov v. Russia*, appl. n° 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324 (URLs last accessed on 18 May 2017).

[250] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., §. 50.

[251] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., §. 51.

[252] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., §. 50.

[253] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., §. 56.

[254] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 3.24, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017), referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051 (last accessed on 12 May 2017); E. Court H. R., Klass and others v. Germany, *op. cit*., §. 55.

[255] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, *op.cit.* §§73 and 75-77 (media surveillance) ; ECtHR, ch., 25 March 1998, *Kopp v. Switzerland*, appl. n°23224/94, §73, http://hudoc.echr.coe.int/eng?i=001-58144 (lawyers surveillance).

[256] *Ibid.*

[257] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, *op.cit.* §§77.

[258] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., § 55.

[259] See for example ECtHR*, Klass and others v. Germany*, *op. cit*., § 56.

Control measures also include rights of access and verification granted to concerned individuals[260], the clarification of the procedure to be followed to exercise these rights[261], including a right of appeal when the right of access is denied[262]…), and - where possible - technical measures ensuring data deletion after a certain period of time[263].

In addition, means must be provided to ensure safeguards effectiveness, such as a judicial organisation and an allocation of resources to ensure the practical possibility and the efficiency of judicial controls.

In conclusion, in order to assess the legitimacy of a measure that will constitute a privacy interference, several questions must be answered:

- Is there a clear, accessible and foreseeable legal basis justifying the interference?
- Does the interference pursue one legitimate aim covered by the ECHR?
- Is the measure necessary?
  - "*Is the measure seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or a section of society?*"[264]
  - *"Is there any evidence that the measure may mitigate such harm?"*
  - *"What are the broader views (societal, historic or political, etc.) of society on the issue in question?"*
  - *"Have any specific views/opposition to a measure or issue expressed by society been sufficiently taken into account?"*
  - What are the existing measures in place? Why are they no longer sufficient and what will be the added value of the proposed measure?
- Is the measure proportionate?
  - Is the proposed measure strictly necessary to achieve the pursued aim?
    - Is it appropriate to its context? (i. e. adapted to the severity of the social need, taking into account the specific crime the measure is intended to address and the harm that crime would cause to society if not addressed; adapted to the

[260] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.,* 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051 (last accessed on 12 May 2017).

[261] See for example ECtHR, 2nd Sect., 24 September 2002, *MG v. the United Kingdom*, appl. n° 39393/98, http://hudoc.echr.coe.int/eng?i=001-60642, and Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 91, available at http://www.cnpd.public.lu/fr/legislation/jurisprudence/cedh/cedh_caselaw_dp_fr.pdf (last accessed on 12 May 2017); ECtHR, *Klass and others v. Germany*, *op. cit*., §. 55.

[262] ECtHR, *MG v. the United Kingdom*, appl. n° 39393/98, *op. cit*.; ECtHR, *Klass and others v. Germany*, *op. cit*., §. 56.

[263] See for example ECtHR, *Klass and others v. Germany*, *op. cit*., §. 52.

[264] This question and the three following ones are proposed by the Article 29 Data Protection Working Party in its Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.19.

nature of the behaviour which is being restricted…);

- Is the scope of the interference sufficiently limited to reach the aim pursued? (in terms of volume of intrusions, number of people affected, situations in which the measure can take place, time during which the measure will be effective…); Does the overall effect of the proposed measure leave some scope for the limited freedom?
- Is the interference, in its nature, the less freedoms-restrictive one? What other measures could be considered, and why are they rejected?

o Is the measure limited by adequate and effective safeguards? (they must clearly define the limits of the interference in order to make the latter compliant with the necessity and proportionality requirements, and define the way these limits will be enforced and controlled, including objective supervision and rights of access/appeal afforded to individuals, not forgetting organisational and financial measures aiming at ensuring their practical effectiveness.

- Are the necessity and the proportionality of the proposed measure sufficiently justified?

  In addition, the information substantiating compliance with the principles of necessity and proportionality must be sufficient to establish convincingly the legitimacy of the interference. This principle is so important that the Article 29 Data Protection Working Party considers this question to be a test in itself, in addition to the necessity test and to the proportionality test.[265] Therefore, it may be important to analyse this question independently, to review the quality and relevance of evidences that have been produced (such as "*research, surveys or other information*"[266]).

4.1.4 Particular challenges posed by the MANDOLA outcomes

All the principles recalled previously in the current report apply to the MANDOLA outcomes. Indeed,

- The monitoring of the spread and penetration of online hate-related speech in the European Union (EU) and in the EU Member States using big-data approaches might have several purposes, including providing policy makers with actionable information that can be used to promote policies for mitigating the spread of online hate speech. Within this framework, it is especially crucial to ensure that there is no disproportionate limitation of citizen's rights. In particular, very few purposes might justify the possibility to track back Internet users' personal data. In addition, great consideration should be given to the impacts of policies that could be operated on the basis of inaccurate or incorrect results.
- The possibility for ordinary citizens to get information on how to behave when facing online hatred and to report such types of content must take care of the preservation of

[265] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.27.

[266] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.27. The working party refers to the ECtHR formula: the "*interference must be supported by relevant and sufficient reasons*". See for example ECtHR, 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. n° 62332/00, § 88, http://hudoc.echr.coe.int/eng?i=001-75591 (last accessed on 12 May 2017).

the anonymity of both citizens and potential perpetrators, where the necessity and the proportionality test do not justify their identification; moreover, advices received must not lead citizens to be mistaken about the actions that are the most appropriate in their specific cases.

- The objective to transfer best practices among EU Member States requires that these practices do not include weaknesses on the privacy preservation area.

These challenges will call for specific scrutiny during the privacy impact assessment (PIA) of the MANDOLA outcomes, in order to ensure that appropriate safeguards are implemented or advised to end-users.

This has been recalled in 2016 by the ECtHR, according to which "*the techniques applied in (...) monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, (...) especially when automated and systemic data collection is technically possible and becomes widespread*"[267]. In this context, "*the development of surveillance methods resulting in masses of data collected*" must be "*accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*"[268].

The court notices that "*these data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like*"[269]. The Court further recalls that even the aim of fighting terrorism, which is not the aim of the MANDOLA outcomes (which will therefore have to be even less intrusive), cannot justify the "*threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives*"[270].

In this context the Court notably recalls that "*large-scale interception (...)* (is a) *matter of serious concern*"[271], as well as "*the possibility occurring on the side of Governments to acquire a detailed profile (...) of the most intimate aspects of citizens' lives*"[272]. Therefore, The PIA of the MANDOLA system will have to ensure that the MANDOLA outcomes cannot feed such operations, and, if they do, to advice for appropriate safeguards.

[267] ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, §68, http://hudoc.echr.coe.int/eng?i=001-160020 (last accessed on 18 May 2017).

[268] *Ibid.,* §68.

[269] *Ibid.,* §68.

[270] *Ibid.,* §68.

[271] *Ibid.,* §69.

[272] *Ibid.,* §70.

4.2 The right to personal data protection

Understanding the right to personal data protection requires addressing the protecting legal instruments of this right, the notion of personal data, and the nature and extent of its protection[273].

4.2.1 Legal instruments protecting personal data

Personal data protection is ensured at the Council of Europe level by the ECtHR on the basis of article 8 of the ECHR, and by the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (known as the "Data Protection Convention" or "Convention n° 108")[274], which is currently subject to proposals for amendments[275]. A recommendation R. (87)15 of the Council of Europe Committee of Ministers applies more specifically to police files[276].

At the European level, the right to personal data protection is declared by Article 8 of the EUCFR, and more precisely protected by the EU Directives 95/46/EC and 2002/58/EC, the latter having been modified by Directives 2006/24/EC and 2009/136/EC. Moreover, a Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters regulates specifically transborder data processing for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. These texts have been implemented into the EU Member States legislations[277].

This EU legal framework has been revised. On 27 April 2016, two legal instruments have been adopted, namely (1) Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (known as the "General Data Protection Regulation" or "GDPR")[278], and (2) Directive (EU) 2016/680 of the

[273] Some elements of the following discussion are coming from Estelle De Marco in Estelle De Marco et al., Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.2, available at https://www.epoolice.eu/.

[274] Convention of 28 Jan. 1981, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (last accessed on 12 May 2017).

[275] See the Council of Europe website, Modernisation of Convention 108, https://www.coe.int/en/web/data-protection/modernisation-convention108 (last accessed on 12 May 2017).

[276] Council of Europe, Committee of Ministers, Recommendation n° R (87) 15 regulating the use of personal data in the police sector, 17 Sept. 1978, available at: https://rm.coe.int/168062dfd4 (last accessed on 12 May 2017).

[277] For example: in France, Law n°78-17 of 6 January 1978 essentially implements Dir. 95/46/EC, and other European provisions are implemented in different laws and codes (for instance the Post and Electronic Communications Code; in Spain, Act 15/1999 of 13 December on the Protection of Personal Data; in Luxembourg, a Law of 2 August 2002 and a Law of 30 May 2005 implement respectively Dir. 95/46/EC and Dir. 2002/58/EC; In Romania, the European texts are implemented in different laws, for example Law n° 677/2001 implements Directive 95/46/EC, Law n°506/2004 implements Dir. 2002/58/EC, and Law n° 238/2009 implements the Council Framework Decision.

[278] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

European Parliament and of the Council on 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (known as "Directive for the police and criminal justice sector"[279] or "Police Directive"[280])[281].

This new EU legislation will only be applicable in May 2018. Indeed, the Regulation will apply two years after its adoption, and the Directive for data protection in the police and justice sectors provides for an implementation period. *"Member States are under an obligation to update their legal frameworks during this time*"[282]. When these instruments will be applicable, the particularity of the Regulation is that it will not have to be implemented into national legislation (as the Directive must be), since it will have a "*binding legal force throughout every Member State, on a par with national laws*"[283].

4.2.2 The notion of personal data

Personal data are data, publicly available or not[284], relating to a natural person who is identified or can be identified directly or indirectly, by any means, for instance "*by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*"[285]. Therefore, **a person is indirectly identifiable when one or several pieces of information held by one or several third parties could, in association with the processed data, lead to the identification of this person**, even if the data controller does not have the necessary resources to make such identification.

---

[279] See for eample European Commission, "Reform of EU data protection rules", http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last accessed on 12 May 2017).

[280] European Commission - Fact Sheet, Questions and Answers - Data protection reform, 21/12/2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (last accessed on 12 May 2017).

[281] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

[282] European Commission - Fact Sheet, Questions and Answers - Data protection reform, 21/12/2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (last accessed on 12 May 2017). See article 99 of the GDPR and article 63 of the Directive for data protection in the police and justice sectors.

[283] European Union website, *Regulations, Directives and other acts*, https://europa.eu/european-union/eu-law/legal-acts_en (last accessed on 12 May 2017).

[284] See for instance Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, III.2.5, pp.35.

[285] See for instance article 2, a, of the Directive 95/46/EC. According to the General Data Protection Regulation, 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" (art.4).

Data that do not longer contain any identifiers are said to be "anonymised"[286]. If the identifiers are encrypted, data are said to be "pseudonymised" and remain personal data[287].

Personal data are considered by some authors as an aspect or "sphere" of private life[288], even if their collection may create risks for other fundamental rights such as non-discrimination and due process[289]. Indeed, on the opinion of these authors, the aforesaid rights may be considered as protected by the secrecy of private life. Furthermore, personal data are protected by the ECtHR under Article 8 of the ECHR which is related to the right to private life[290].

The legal authors who consider that personal data and privacy are two spheres that overlap without being exactly the same, argue notably, in addition to note the other fundamental rights limitations that may occur when processing personal data, that these personal data may be related to elements of the public life of an individual, and therefore to information that is not related to privacy[291].

This being said, the question to know whether personal data are an aspect of privacy or are forming a sphere which overcomes privacy boundaries is a debate which is not of

---

[286] For an analysis of the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection, see the Article 29 Data Protection Working Party's opinion on anonymisation techniques, 10 April 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 12 May 2017).

[287] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data protection law, December 2013, p. 36, available at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 12 May 2017). See also the European Parliament legislative resolution of 12 March 2014 on the General Data Protection Regulation, *op. cit*., which proposes definitions for pseudonymous data and encrypted data.

[288] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p.42; Ahti Saarenpää, "Perspectives on privacy", in Ahti Saarenpää, *Legal privacy*, LEFIS Series, 5, Prensas Universitarias de Zaragoza, p. 21 (http://puz.unizar.es/detalle/898/Legal+privacy-0.html), accessible at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf (last accessed on 12 May 2017): "*Thus, when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone*". P. 23, this author also notices that "*In the United States, Canada, Australia and New Zealand, for example, legislation enacted under the heading 'privacy' deals primarily with the processing of personal data*". See also F. M. Rudinsky, *Civil Hulan Rights in Russia - Modern Problems of Theory And* Practice, Transaction Publishers, 2008, p. 40: "*The constitutional term "secret" expresses inadmissibility of illegal and unreasonable penetration into the sphere of individual freedom with a view of illegal acquirement of personal information of a citizen against their will*".

[289] Mireille Hildebrandt, and Bert-Jaap Koops, "The challenges of Ambient Law and legal protection in the profiling era", May 2010, Modern Law Review 73 (3), p. 428-460.

[290] See notably on this issue Ahti Saarenpää, "Perspectives on privacy", *op.cit.*, p. 22:"*Articles 7 and 8 of The Charter of Fundamental Rights of the European Union distinguish between private life and the processing of personal data. This reflects the view embodied in the 1995 Personal Data Directive whereby protection of personal data is an aspect of the protection of privacy. Article 1 of the Directive expresses the situation clearly: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*'".

[291] See for instance Paul De Hert Dariusz Kloza, David Wright and all., *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.14, available at http://www.piafproject.eu/Deliverables.html (last accessed on 12 May 2017).

the utmost importance within the framework of our study. Indeed, the legal instruments that will base the legal assessment of the MANDOLA project cover both the protection of privacy and the protection of personal data:

- The protection offered by the ECtHR to both private life and personal data is of the same nature, as we will analyse it, and is based on the same provision (art. 8 of the ECHR;
- The EU legislation protecting personal data do not distinguish between data that would be private and data of other nature.

It should also be noted that the definition of privacy proposed in the present study allows considering personal data as being included in the private zone of the individual.

4.2.3 Nature and extent of the personal data protection

The nature and extent of the protection of personal data will be studied in the light of the EU legislation, without taking into account the specificity of the legislations of each EU Member States (only some examples might be given). Indeed, such a comparative analysis would be counter-productive, taking into account the upcoming modifications that will be induced by the new EU legal framework.

The study of the nature and extent of the protection of personal data implies to analyse the material scope of the protection, the territorial scope of the protection and the substance of the protection.

4.2.3.1 Material scope of the protection

The personal data protection may differ, especially in the EU legislation, according to the purposes of the processing, according to the processing techniques that are used or according to the activity of the data controller.

4.2.3.1.1 The protection may differ according to the purposes of the processing

At the Council of Europe level, the requirements of the ECHR and of the Data Protection Convention apply to all personal data processing whatever the purpose, and particularly to police files or to so-called "sovereign' files" or "intelligence files"[292].

For its part, as already mentioned, Recommendation R 87(15) of the Committee of Ministers of the Council of Europe applies only to personal data processing for police purposes, since

[292] Regarding the ECtHR, see for instance ECtHR, gr.ch., 4 May 2000, ECtHR, gr.ch., *Rotaru v. Roumania*, appl. n°28341/95, http://hudoc.echr.coe.int/eng?i=001-58586; ECtHR, 3rd Sect., 27 October 2009, *Haralambie v. Romania*, appl. n°21737/03, http://hudoc.echr.coe.int/eng?i=001-95302; Regarding the EU, see for instance the CJEU court case Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, 8 April 2014, §40, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12; Regarding the Data Protection Convention, see notably Council of Europe Committee of Ministers, explanatory memorandum to Recommendation n° R (87) 15, available at https://rm.coe.int/168062dfd4 (URLs last accessed on 12 May 2017).

this recommendation aims to adapt the Data Protection Convention[293] and the ECHR principles[294] to the specific requirements of the police sector.

At the European Union level, the requirements of the EUCFR apply to all personal data processing whatever the purpose, while Directives 95/46/EC and 2002/58/EC do not apply to the processing of personal data in the course of activities which fall outside the scope of Community law[295], such as those provided by Titles V and VI of the Treaty on the European Union (respectively article 3, 2 and 1, of the directives), and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law[296]. Therefore, they notably not apply to the issue of access to data by the competent national law-enforcement authorities and to the issue relating to the use and exchange of those data between those authorities[297].

In the same line, when a data processing falls within the scope of Directive 95/46/EC, but the data processed are further needed to safeguard some interests exhaustively listed in article 13 of the Directive, including the detection and prosecution of criminal offences, Member States are allowed to adopt legislative measures to restrict the scope of some obligations and rights provided for in the Directive. Such a restriction is however optional[298].

Therefore, the Council Framework Decision 2008/977/JHA of 27 November 2008 is the only obligatory EU text relating to processing operations for police purposes, beyond the principles mentioned in the EUCFR, and this text targets only transborder data processing for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty.

More specifically, this Council Framework decision does only apply when personal data (a) are made available between Member States, (b) are made available by Member States to authorities or to information systems established on the basis of Title VI of the Treaty on European Union which makes provisions on police and judicial cooperation in criminal matters[299], or (c) are made available to the competent authorities of the Member States

[293] Council of Europe Committee of Ministers, explanatory memorandum to Recommendation n° R (87) 15, *op. cit*, n° 1 *et seq*.

[294] Council of Europe Committee of Ministers, explanatory memorandum to Recommendation n° R (87) 15, *op. cit*., n°6, 16, 17, 20.

[295] Article 3 of Directive 95/46/EC; Article 1 of Directive 2002/58/EC.

[296] Article 3 of Directive 95/46/EC; Article 1 of Directive 2002/58/EC.

[297] European Court of Justice, *Ireland v. European Parliament and Council of the European Union*, 10 February 2009, Case C-301/06.

[298] Judgment of the Court (Third Chamber) of 7 November 2013 (request for a preliminary ruling from the Cour constitutionnelle — Belgium) — *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, Case C-473/12, Operative part of the judgment in OJEU of 11/01/2014, C9/14, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2014:009:0013:0014:EN:PDF, decision in French language available at https://www.legalis.net/jurisprudences/cour-de-justice-de-lunion-europeenne-3eme-chambre-arret-du-7-novembre-2013/ (URLs last accessed on 12 May 2017).

[299] A Table of equivalences between the old numbering and the new numbering of the Treaty on European Union is available in the consolidated versions of the treaty on European Union and the treaty on the

by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community[300].

However, the existence of this text and of Recommendation R. (87)15 of the Committee of Ministers of the Council of Europe[301], together with the necessity for police files to respect the ECHR and the EUCFR[302], may explain that "*in most Member States the scope of the implementing legislation is wider than the directive (95/46/CE) itself requires and does not exclude data processing for the purpose of law enforcement*"[303]. This is for example the case in France[304], Spain[305], Romania[306] and Greece[307].

In addition, the situation will change when the new Directive for data protection in the police and justice sectors will be applicable. Indeed, this Directive still does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law[308], but it applies 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[309]. It includes many principles that are common with the General Data Protection Regulation, thereby strengthening citizens' personal data protection.

---

functioning of teh European Union, March 2010, pp.361 et seq., available at https://europa.eu/european-union/sites/europaeu/files/eu_citizenship/consolidated-treaties_en.pdf (last accessed on 12 May 2017).

[300] Article 1 of the Council framework decision, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF (last accessed on 12 May 2017).

[301] This recommendation is not formally binding for the countries that are parties to the ECHR. However, the Committee of Ministers recommendations are related to actions required to further the aim of the Council of Europe and the European Convention on Human Right. In that sense, Member States that took the commitment to respect the ECHR should follow the Committee of Ministers recommendations. See the statute of the Council of Europe (available at http://conventions.coe.int/Treaty/EN/Treaties/Html/001.htm - last accessed on 12 May 2017), and Alexandre-Charles Kiss, *Annuaire français du droit international*, Year 1960, Volume 6, pp. 755-773, notably pp. 765 and 766.

[302] As we will analyse it below, the principles established by the EU legal instruments and the Committee of Ministers' recommendation may be seen as ways to ensure the ECtHR more general principles (legal basis, legitimate purpose, necessity and proportionality), in most situations where personal data are processed. Some of these ways are moreover recognised as fundamental rights in the EUCFR.

[303] Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final, 19 December 2005, §4, available at http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf (last accessed on 12 May 2017).

[304] Law n° 78-17 of 6 January 1978 also applies to law enforcement activities.

[305] Art. 22 of the Act 15/1999 of 13 December on personal data protection regulates specifically law enforcement activities.

[306] Law 677/2001 on personal data protection also applies to law enforcement activities (art. 2).

[307] Law 2472/1997.

[308] Article 2 of the Directive for data protection in the police and justice sectors (Directive (EU) 2016/680).

[309] Article 1 (1) of Directive for data protection in the police and justice sectors (Directive (EU) 2016/680).

4.2.3.1.2 The protection may differ according to the processing techniques

The requirements of the EUCFR and of the ECHR apply to every kind of personal data processing.

Recommendation R 87(15) of the Committee of Ministers of the Council of Europe applies to personal data automatic processing for police purposes, while it enables Member States to extend the principles contained in this text to personal data not undergoing automatic processing and states that manual processing should not take place if the aim is to avoid the provision of the Recommendation.

Directives 95/46/EC and 2002/58/CE both "*apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*". The scope of the future EU legal framework will be the same[310].

4.2.3.1.3 The protection may differ according to the activity of the data controller

While the other legal instruments targeted above apply to any data controller, with a specificity for police files, Directive 2002/58/EC applies more specifically to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, according to its article 3.

> Literally, this means that the Directive is supposed to apply only to the processing of personal data by operators of electronic communications and by Internet access providers, since the notion of "*provision of electronic communications services*" relates, in the EU legislation and in national legislations as the French one, respectively to the "transmission"[311] and to the "transport"[312] of data, and such transmission or transport is ensured by operators. In consequence, article 3 of Directive 2002/58/EC declares that this Directive does not apply to stakeholders that would not transport electronic communications. Nonetheless, as we will analyse it below (see, in relation with the substance of the protection, the subsection relating to the enhanced protection of some sensitive data), some provisions of the Directive apply to every kind of data controllers (either on the basis of a contradictory article of the Directive, or on the basis of Directive 95/46/EC as interpreted by the Article 29 Data Protection Working Party).

In addition, all the above-mentioned texts apply to activities that are not exclusively carried out by a natural person in the course of a purely personal or household activity. Indeed, in the latter case, their application is explicitly excluded[313].

---

[310] Article 2 of the GDPR and article 2 of the Directive for data protection in the police and justice sectors.

[311] Directive 2002/21/EC, art. 2, c (directive that has been modified by Directive 2009/140/EC).

[312] See Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN: 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 266 *et seq.*; in the same line see ARCEP, *Etude sur le périmètre de la notion d'opérateur de communications électroniques*, study prepared by the firms Hogan Lovells et Analysys Mason for the ARCEP, June 2011, not. p. 46, http://www.arcep.fr/uploads/tx_gspublication/etude-Hogan-Analysys-juin2011.pdf (last accessed on 12 May 2017).

[313] Article 2 of the GDPR.

4.2.3.2 Territorial scope of the protection

Regarding territorial application, the ECHR applies in the 47 countries that are parties to this Convention, including all the EU Member States, as well as Recommendation R 87(15) of the Committee of Ministers of the Council of Europe. The Data Protection Convention applies in 45 countries[314].

At the European level, the EUCFR applies in all the EU Member States and each national law that results from the transposition of Directives 95/46/EC and 2002/58/EC only applies when the data controller is established on the territory of the concerned Member State, when the controller is established in a country where the law of the concerned State applies, or when this controller processes personal data using an equipment located on the territory of the said Member State[315], which will be the case if this controller uses calculating facilities, java scripts, or cookies on the user's terminal located in the concerned Member State to store and retrieve personal data[316].

This will change with the application of the new EU legal framework. Indeed, the GDPR[317] applies:

- to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not; to data controllers or processors who are established in the union;
- and to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Conclusion on the material and territorial scope of the protection:

Personal data processing operated by the MANDOLA consortium and those that would be operated by other natural or legal persons (other than competent authorities acting in crime prevention or repression) as a result of the use of the MANDOLA outcomes should respect the ECHR, the EU charter on Fundamental Rights, the Council of Europe Data Protection Convention, the EU Directives 95/46/EC and 2002/58/EC, and the national legislation implementing these Directives in the Member State in which the data controller is established. These processing operations may have, in the future, to comply with the new General Data Protection Regulation.

[314] The Convention applies in all the countries that are members of the Council of Europe except Turkey and San Marino, and applies in Uruguay, which has ratified the Convention although it is not a member of the Council of Europe. See the Council of Europe website, regarding the status of the Convention, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?CL=ENG&CM=&NT=108&DF=&VL= (last accessed on 12 May 2017).

[315] Article 4 of Directive 95/46/EC.

[316] Data Protection Working Party, Opinion 8/2010 on applicable law, 16 December 2010, WP179.

[317] Article 3. The GDPR also applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Personal data processing that would be operated by LEAs, as a result of the use of the MANDOLA outcomes, should be compliant with the provisions of the ECHR, the Council of Europe Data Protection Convention, and Rec. (87) 15 of the Committee of Ministers of the Council of Europe[318], in the countries that are parties to the afore mentioned Conventions, which include all the EU Member States. Personal data processing operated by LEAs in EU Member States should also comply with the provisions of the EU charter on Fundamental Rights, and, in the perspective of transborder data processing[319], with the provisions of the Council Framework Decision 2008/977/JHA. These processing should moreover comply with the national laws implementing these EU instruments, and with some of the provisions of Directive 95/46/EC, since in most EU Member States the scope of the implementing legislation does not exclude data processing for the purpose of law enforcement. In addition, personal data processing operated by EU LEAs will have, in the future, to comply with the new Directive for data protection in the police and justice sectors.

4.2.3.3 Substance of personal data protection

Firstly, any personal data processing - including when operated by LEAs - shall respect the principles of legal basis, of legitimate purpose, of necessity and of proportionality stated in the ECHR and the EUCFR[320]. When it relates to personal data, article 7 (relating to privacy protection) and article 8 (relating to personal data protection) of the EUCFR should be read jointly due to the inter-relation between the rights they recognise[321].

Secondly, any personal data processing must respect the more specific principles and rules contained in the Data Protection Convention, the EU Directives, the Council Framework Decision 2008/977/JHA and / or the Recommendation R. (87)15 of the Committee of Ministers of the Council of Europe (Rec. 87 (15) below), and naturally the national laws implementing these European or international legal instruments, when it falls within their scope of application.

These more specific principles and rules may be seen, for the most part, as practical ways to ensure compliance - according to the Council of Europe (CoE) Member States[322] or to the EU

[318] All the EU Member States are party to the ECHR, and the ECtHR is always likely to retain the liability of one of these Members States for not complying with Rec (87) 15, since this recommendation aims at adapting the E. Conv. H. R. principles, in addition to adapting the Data Protection Convention ones, to the specific requirements of the police sector.

[319] Council Framework Decision 2008/977/JHA must be respected in all the EU Member States within the framework of transborder data processing for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. Therefore, it may be important for police files to be compliant with this decision with the framework of the use of MANDOLA outcomes, online hate speech being border-free.

[320] See above our section dedicated to the content of the right to private life protection.

[321] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, p. 4, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[322] Through their representatives, namely Foreign Affairs Ministers. See Council of Europe website, "What is the Committee of Ministers (CM)?", available at http://www.coe.int/t/cm/aboutcm_EN.asp? (last accessed on 12 May 2017).

legislator - with the ECHR and the EUCFR principles, within the framework of most data processing operations.

This means that, on the first hand, these specific rules must be interpreted in the light of these more general principles, including the principles of necessity and proportionality[323], and, in the other hand, that **some processing may have to be based on additional specific legislation, to be compliant with the ECHR and the EUCFR** (principle of legal basis). **Such a specific legislation may have to implement additional appropriate safeguards, when generic ones are not sufficient or are not suitable** for ensuring the legitimacy of the targeted processing operations.

In this sense, the Data Protection Convention, the EU Directives, the Council framework decision and the Recommendation of the Council of Europe's Committee of Ministers advocate the adoption of additional specific laws containing further appropriate safeguards, to regulate some processing they consider as particularly sensitive[324].

> These more specific provisions use sometimes the term "necessary" (mentioning for example a "necessary" measure), as we will analyse it below. This term "necessary", used in the EU data protection legislation, should be understood as referring to the principle of necessity laid down in the EU Charter of Fundamental Rights, which, itself, has the same meaning as the ECHR formula: "*necessary in a democratic society*" (which contains the principles of necessity and proportionality that we analysed in Section 4.1.3), as highlighted by the Article 29 Data Protection Working Party[325].[326]
>
> This leads to provide an additional safeguard that thereby *"limits any data processing"* targeted in the provisions in question[327].
>
> Such an interpretation is in line with the "*need for a consistent approach*" to the application of the principle of necessity "*and its impact on data protection*",

---

[323] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, Part V, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 27 March 2014).

[324] See *infra*.

[325] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 4.2.

[326] For an example of decision of the CJEU in that sense, see the CJEU case C-465/00 and C-138/01, *Rechnungshof v. Osterreichischer Rundfunks*, 20 May 2003, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dee4d1b40948404f1c87fcdbf9dd4d2d3a.e34KaxiLc3eQc40LaxqMbN4OaNyTe0?text=&docid=48330&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=162751. See also, in relation with this case, Laraine Laudati, *EU court decisions relating to data protection*, December 2012, http://ec.europa.eu/anti_fraud/documents/data-protection/dpo/ecj_decisions_relating_data_protection_en.pdf (last accessed on 2 May 2014): "*But "necessary" means that a pressing social need is involved and the measure is proportionate to the legitimate aim pursued. The authorities enjoy a margin of appreciation. The interests of the state must be balanced against the seriousness of the interference. The interference is justified only insofar as publication of the names is both necessary and appropriate to the aim of keeping salaries within reasonable limits, which is for the national court to examine. If not, then the interference also constitutes a violation of Articles 6 and 7 of Directive 95/46*".

[327] *Ibid.*

particularly with regards to data processing in the Justice and security contexts, which has been highlighted by the EUCJ. Indeed, the EUCJ states: "*Having regard to the objective of Directive 95/46/EC of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Art. 7(e) of the directive cannot have a meaning which varies between the Member States*"[328].

All these more specific principles and rules, to be respected when collecting or processing personal data, may be divided into fourteen categories of principles that are common to the four above-mentioned EU and CoE instruments to a greater or lesser extent, and some of them are strengthened, for a better protection of the individual, within the framework of the new EU framework, including in cases where personal data are processed by LEAs. Some of these more specific principles and rules are moreover recognised as fundamental rights by the EUCFR.

The fourteen general principles that are common to the EU Directives, to the Data Protection Convention (or to the proposals for modification of this Convention), to Rec (87) 15 and to Council Framework Decision 2008/977/JHA, are the following:

4.2.3.3.1 - Legal basis

A legal basis must regulate personal data processing operations. This principle is a requirement of the ECHR[329] and of the EUCFR[330], and is more or less implicitly reminded in the other international and European legal instruments[331]. This legal basis must meet the quality criteria developed by the European Court of Human Rights[332].

This legal basis is commonly the national law implementing international or European texts and authorising data processing under strict conditions, which consist in respecting the other principles listed below.

Some personal data processing operations are moreover prohibited or cannot take place if they are not authorised by an additional law providing for specific and adequate safeguards (i.e. safeguards going farer that the generic national law).

---

[328] *Ibid.*

[329] Art. 8, 2 of the Convention.

[330] Art. 52.1 of the Charter.

[331] **The Data Protection Convention** lays down that "*Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter*" (art. 4), and that "*Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out*" in its chapter II; **Directive 95/46/EC** lays down that "each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data" in the situations listed in article 4 (art. 4);

[332] See for instance the Article 29 Data Protection Working Party opinion 03/2013 on purpose limitation (WP 203), 2 avril 2013, p. 38, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed on 20 March 2014): "*a qualified test must be applied, to ensure that the legislative measure meets the criteria that allow derogating from a fundamental right. There are two aspects to this test: on the one hand the measure must be sufficiently clear and precise to be foreseeable, and on the other hand it must be necessary and proportionate, consistent with the requirements developed by the EUropean Court of Human Rights*"; see also European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data protection law, December 2013, p. 64-66, available at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 17 April 2014).

In the field of police processing, personal data processing operations that need to be authorised by a specific law are mainly the following one:

1. **The processing of sensitive data** (personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of data concerning health or sex life*"); In this case the national law must provide for "*adequate safeguards*" [333].
2. **The authorisation to take "*a decision which produces an adverse legal effect for the data subject* or *significantly affects him (or her)* *and which is based solely on automated processing of data* *intended to evaluate certain personal aspects relating to the data subject*"[334] (including profiling[335]). In such a case, law must lay down appropriate safeguards for "*the data subject's legitimate interests*"[336]).
3. **Any collection of personal data for police purposes that would not be limited to "*such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence*"**[337]. The term "*necessary*", in this sentence from the Council of Europe Committee of Ministers, should be understood as referring to the principles of necessity and proportionality developed by the ECHR[338].

   The wording used in the 2016 Directive for data protection in the police and justice sectors is wider[339]; however, the ECHR principles of necessity and proportionality impose, as already analysed in Section 4.1.3 of the current study, a reading of its provisions in line with the Council of Europe Committee of Ministers' recommendation.

   In addition, the 2016 Police Directive recalls in its article 8 that all personal data processing 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, must be necessary to the fulfilment of these purposes and must be authorised by a national or a EU law specifying "*at least the objectives of processing, the personal data to be processed and the purposes of the processing*". Once again, the provisions of this Directive should be read in conjunction with the ECHR principles, and their interpretation by the ECtHR. This

[333] Council Framework Decision 2008/977/JHA, Article 6. The Data Protection Convention (article 6), which is applicable both to the private and to the public sector, also prohibits the automatic process of special categories of data "unless domestic law provides appropriate safeguards"; Article 10 of the Directive for data protection in the police and justice sectors (which refers to "appropriate safeguards)..

[334] Council Framework Decision 2008/977/JHA, Article 7.

[335] Directive for data protection in the police and justice sectors, article 11.

[336] Council Framework Decision 2008/977/JHA, article 7; art. 11 of the Directive for data protection in the police and justice sectors evoke "*appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller*".

[337] Appendix to Recommendation R (87) 15, Principle 2.1.

[338] See above the introduction of the current section.

[339] Article 9 of the Directive: personal data processing that must be authorised by law are those which purposes are "other than those set out in Article 1" (i.e. 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).

latter court has ruled that the legal basis (authorising a processing, in our current case) must "*indicate the scope and manner of exercise of any (limitation of right) with sufficient clarity (...) to give the individual adequate protection against arbitrary interference*"[340]. This statement imposes, as a consequence, that the law authorising the processing specifies also clearly the safeguards to be implemented in order to safeguard data subjects' rights, where such safeguards are needed.

4. **The collection of data by technical surveillance or other automated means**[341]. The 2016 Police Directive does not explicitly imposes a specific law in this case, but only imposes a data protection impact assessment (DPIA) where the processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" (taking into account its "*nature, scope, context and purposes*")[342], and, in case of high risk (which will particularly be the case where new technologies, mechanisms or procedures are used[343]), a prior consultation of the supervisory authority[344]. However, as already analysed, the Police Directive must be read in conjunction with the ECtHR opinion recalled in paragraph n°3 above. As a result, and since the DPIA must contain the measures and safeguards envisaged to address the risks posed by the processing[345], and that these safeguards constitute a crucial part of the protection of the individual against arbitrary interference, a full respect of the legal framework implies that the national or EU[346] legislation authorising the processing imposes the implementation of the safeguards proposed as a outcomes of the DPIA.
5. **The introduction of new technical means for data processing**[347]. The text does not impose the adoption of a specific law but requires States to "*ensure*" that the use of such means "*complies with the spirit of existing data protection legislation*". However, the first guardians of civil rights and freedoms at the domestic level are the Parliament and the judiciary. Due to the relative effect of judgments, the compliance of data processing operations with the spirit of the legislation implies primarily a legal adaptation of this legislation to the particularity of the targeted operations. In addition, the provisions of the Police Directive recalled in the preceding paragraph, and our analysis of these provisions, fully apply to the introduction of new technical means for data processing.
6. "**Direct access/online access** to a file": in this case, the national law must take account of several principles such as data quality, data minimisation, purpose, transparency,

[340] Council of Europe, Case law of the European court of Human rights concerning the protection of personal data, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19, http://www.cnpd.public.lu/fr/legislation/jurisprudence/cedh/cedh_caselaw_dp_fr.pdf, in relation to ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, http://hudoc.echr.coe.int/eng?i=001-57533. See Section 4.1.3 for more precise references.

[341] Appendix to Recommendation R (87) 15, Principle 2.3.

[342] Art. 27 of the Directive for data protection in the police and justice sectors.

[343] *Ibid.*

[344] Art. 28 of the Directive for data protection in the police and justice sectors.

[345] Art. 27 of the Directive for data protection in the police and justice sectors.

[346] Art. 8 of the Directive for data protection in the police and justice sectors.

[347] Appendix to Recommendation R (87) 15, Principle 1.2.

data subjects' rights, and rules governing the communication of data[348]. On the same line, the provisions of the Police Directive recalled in paragraph 4 above, and our analysis of these provisions, fully apply to direct or online access to personal data.

7. **The collection of personal data on social networks**[349], which implies several operations already listed above.
8. **The exclusion of a written statement** (which may only occur "*in specific cases*"), **in situations where "*the data subject exercises its right of access*"**[350]. The new Police Directive, for its part, also imposes a written statement in case the data subject exercises his or her right of access[351]. In addition, the Directive lists the information that the data subject must receive in such case[352], and the principle of controller's accountability[353] ensures that the information is received. Moreover, the Directive imposes the adoption of a specific law in order to authorise any limitation to the right of access[354], as well as any limitation of the data subject's right to information before any request in this sense[355].

In certain other cases, the measure must be authorised either by a specific law, or by the supervisory authority:

- **Communication of data to other public bodies than police services, or to private parties**, "*if these data are not indispensable to the recipient or if these data are indispensable but the aim of the processing to be carried out by the recipient is not compatible with the original processing or if the legal obligations of the communicating body are contrary to this*"[356]. To be noted that such a communication is prohibited by the new Police Directive (since the processing must be "necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1" of this Directive[357]), which means in practice that only a specific law providing for appropriate safeguards might authorise it.
- **The "*interconnection of files with files held for different purposes*"**: the authorisation of the supervisory authority can only be given "*for the purpose of an inquiry into a particular offence*"[358]. As regards the other situations and within the

[348] Appendix to Recommendation R (87) 15, Principle 5.6.

[349] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 April 2012, §15, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)4&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 (last accessed on 21 April 2014).

[350] Appendix to Recommendation R (87) 15, Principle 6.4.

[351] Art. 12 and art. 14 of the Directive for data protection in the police and justice sectors.

[352] Art. 14 of the Directive for data protection in the police and justice sectors.

[353] Especially articles 4 (4), 19 and 25 of the Directive for data protection in the police and justice sectors.

[354] Art. 15 of the Directive for data protection in the police and justice sectors.

[355] Art. 13 of the Directive for data protection in the police and justice sectors.

[356] Appendix to Recommendation R (87) 15, Principles 5.2 and 5.3.

[357] Art. 8 of the Directive for data protection in the police and justice sectors.

[358] Appendix to Recommendation R (87) 15, Principle 5.6.

framework of the application of the new Police Directive, a specific law might be needed since its provisions recalled in paragraph 3 above, and our analysis of these provisions, fully apply to the interconnection of files held for different purposes.

In addition, the new Police Directive authorises the processing for police purposes[359] **of data initially processed for other purposes,** if the processing of such data for police purposes is authorised by law and if this processing is necessary and proportionate to the pursued police purpose[360].

To be noted that, as shown above, this new Directive clarifies the condition of legal basis required by the ECtHR, and provides in addition for certain guidelines in terms of compliance with the other principles of legitimate purpose, necessity and proportionality[361], even if it could have been more detailed on certain aspects[362].

Conclusion on the principle of legal basis:

The MANDOLA consortium, during the course of its research, as well as **other natural or legal persons (other than competent authorities acting in crime prevention or repression) who will process personal data as a result of the use of the MANDOLA outcomes,** must respect the generic data protection law. This means more precisely that data controllers must respect their respective national law transposing the EU directives, and the potential specific safeguards developed in this national law. They will need, in 2018, to comply with the General Data Protection Regulation and the changes that will be brought to their legislation accordingly.

Personal data processing that would be operated by LEAs, as a result of the use of the MANDOLA outcomes, should be compliant with a specific EU or national law authorising the processing and providing for specific and relevant safeguards, if their processing operations may be classified in one or several of the above-mentioned categories (under both the current and the future legislation if not otherwise specified below):

- Processing of sensitive data;
- Authorisation to take a decision which produces an adverse legal effect for the data subject or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or

[359] Which means for the purpose 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", article 1 (1) of the Directive.

[360] Article 4 (2) of the Directive for data protection in the police and justice sectors.

[361] See above our Section 4.1.3.

[362] See for example above the paragraphs n°3 and n°4 of the current section, showing that some conclusions on legal requirements are only found by reading the Directive in the light of the ECHR requirements. See also Estelle De Marco, in Estelle De Marco et al., Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.2.3 (on https://www.epoolice.eu/), which analyses the draft law of the Police Directive has it had been amended by the European Parliament on 12 March 2014 (and which was regulating police files more strictly on some aspects, thereby respecting more closely the ECHR).

her (including profiling);

- Any collection of personal data for police purposes that would not be limited to "such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence";
- Collection of data by technical surveillance or other automated means;
- Introduction of new technical means for data processing;
- Direct access/online access to a file;
- Collection of personal data on social networks;
- Exclusion of a written statement in situations where the data subject exercises its right of access. When the Police Directive will be applicable, any limitation to the right of access or to the right to information will impose the adoption of a specific law;
- Communication of data to other public bodies than police services, or to private parties (a DPA authorisation might be enough before the application of the new Police Directive);
- The interconnection of files with files held for different purposes (a DPA authorisation might be enough before the application of the new Police Directive in case it only feeds the purpose of an inquiry into a particular offence).

Further, in order to comply with the ECHR and to anticipate the application of the new Police Directive, all these processing should be based on a law specifying at least the objectives of processing, the personal data to be processed, the purposes of the processing, and the safeguards to be implemented in order to safeguard the rights of the data subjects.

4.2.3.3.2 - Legitimate, explicit, specified purpose and compatible use

This requirement is included in all legal instruments. Its meaning has been clarified by the Article 29 Data Protection Working Group, and it requires the performance of a compatibility test in case of further processing, including in case of further processing for scientific purposes.

4.2.3.3.2.1 A requirement from all legal instruments

According to Directive 95/46/EC, data must be "*collected for specified, explicit and legitimate purposes and not further processed in way incompatible with these purposes*"[363] (principle of "compatible use"). These principles are taken up in very close terms in the new General Data Protection Regulation and Police Directive.

These principles are also contained in the Data Protection Convention[364], in the Council Framework Decision 2008/977/JHA[365] and in Recommendation R. (87)15 of the Council of

[363] Article 6 (b) of Directive 95/46/EC.

[364] The Convention does however not include explicitly the requirement of "explicit" purpose.

[365] According to Article 3 of the Council Framework decision, "*further processing for another purpose shall be permitted is so far as (a) it is not incompatible with the purposes for which the data were collected, (b) the competent authorities are authorised to process such data for such other purpose in accordance with the*

Europe Committee of Ministers[366]. Most of all, these principles meet the requirements of the E. Court H. R., which imposes a specific, clear, foreseeable and accessible legal basis detailing, *inter alia*, the "*grounds required for ordering*" the measures that constitute the interference[367].

Therefore, these principles are to be respected by the MANDOLA consortium during the course of its research, and by LEAs and other natural or legal persons who may process personal data as a result of the MANDOLA outcomes.

To be noted that - as already said[368] - the new Police Directive authorises the processing for police purposes[369] of data initially processed for other purposes, if the processing of such data for police purposes is authorised by law and if this processing is necessary and proportionate to the pursued police purpose.[370]

4.2.3.3.2.2 Meaning of the notions

As regards the meaning of the notions of "specified", "explicit" and "legitimate" purpose, and of the notion of "compatible use", the Article 29 Data Protection Working Party Opinion should serve as a reference, since it aims to "*ensure a common understanding of the existing legal framework*"[371] in a context where a lack of harmonisation is noticed between Member States[372]. Indeed, the principle of purpose limitation contributes to "*transparency, legal certainty and predictability*"[373], but also to data minimisation and therefore to

---

applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose". Moreover, according to Article 11, when data are received from another Member State, they can only be further processed for a restricted list of purposes other than those for which they were transmitted (these purposes are the following: prevention, investigation, detection or prosecution of criminal offences; execution of criminal penalties; other judicial and administrative proceedings directly related to one of the aforementioned purposes; prevention of an immediate and serious threat to public security; any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law).

[366] The text does not mention the obligation of purpose legitimacy, but declares in its preamble to bear in mind the Data Protection Convention and the provisions of Article 8 of the ECHR, which both lay down the principle of purposes' legitimacy, and limits the authorised purposes to the "prevention of a real danger" and to "the suppression of a specific criminal offence", any other purpose being only allowed if subject to a specific national legislation (Appendix to Recommendation R (87) 15, Principle 4). Rec. 87 (15) moreover states that "personal data collected and stored by the police for police purposes should be used exclusively for those purposes", subject to the principles regulating data communication (ibid).

[367] See for example ECtHR, *Klass and others v. Germany*, *op. cit*., §. 50.

[368] See above, the principle of legal basis.

[369] Article 4 (2) of the Directive for data protection in the police and justice sectors.

[370] Which means for the purpose 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", article 1 (1) of the Directive.

[371] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, I, p.6.

[372] The Article 29 Data Protection Working Party stressed that "*lack of harmonised interpretation has led to divergent applications of the notions (…) in the different Member States, especially in comparison to other principles*": *Ibid*, I, p. 5.

[373] *Ibid*., II.2, p.11.

proportionality. In this sense, it "*is an essential condition to processing personal data and a prerequisite for applying other data quality requirements*"[374]. Basically, these principles should be understood as follows:

Purpose legitimacy

As highlighted by the Article 29 Data Protection Working Party, "*the requirement of legitimacy means that* ***the purposes must be 'in accordance with the law' in the broadest sense****. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts*"[375].

Purpose specification

Each separate purpose must be "*sufficiently defined*", prior to the time of the data collection, "*to delimit the scope of the processing operation"* and therefore to enable the assessment of the compliance of the data collection with the law and to enable the "*implementation of any necessary data protection safeguards"*[376]. This specification requires "*an internal assessment*" to identify and detail the kind of processing that "*is and is not included within the specified purpose*"[377] Purposes too vague such as "*improving users' experience*" or "*IT-security purposes*" are usually not specific enough. In the same line, an overall purpose used to cover a number of separate purposes is not compliant[378].

Explicit purpose

The purpose must be "*sufficiently unambiguous and clearly expressed*"[379], "*in such a way so as to be understood in the same way*" by the data controller and its staff including third parties processors, the supervisory authority and the data subjects[380]. This principle enables therefore all the parties "*to have a common understanding of how the data can be used*", and reduces the risk to process data for a purpose that is not expected by the data subject[381], which is one of the requirements ensuring proportionality, according to the ECtHR[382]. It also enables data subjects to make informed choices[383], which is a freedom of private life[384]. Several forms of complying with this requirement do exist (notices, notification to the data protection authority…), and certain national legislations provide for

[374] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op.cit*., II.2, p.11.

[375] *Ibid.*, III.1.3, p.20.

[376] *Ibid*., II.2.1, p.12 and III.1.1 p. 16.

[377] *Ibid*., III.1.1, p.15.

[378] *Ibid.,* III.1.1, p.16.

[379] *Ibid.,* II.2.1, p.12.

[380] *Ibid.*, III.1.2, p.17.

[381] *Ibid*.

[382] See *supra* Section 4.1.3, under "the proportionality of the very behaviour which is being restricted", in relation with the data subject's expectation of privacy.

[383] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op.cit*., III.1.2, p.17.

[384] See *supra*, Section 4.1.2.

guidelines in that area[385]. The important thing is "*the quality and the consistency of the information provided*"[386], in addition to its accessibility.

Compatible use

Once the data are collected, any other processing must not be incompatible with this first processing, whether or not it has the same purpose[387]. It is necessary to note that applying an anonymisation technique constitutes a further processing, which means that such an operation implies on the first hand that the personal data have been first collected in compliance with law, and on the other hand that such an anonymisation needs to be compliant with the principle of compatible use[388].

To assess this compatibility, the Article 29 Data Protection Working Party recommends to adopt a substantive method, which consists in going "*beyond formal statements to identify both the new and the original purpose, taking into account the way they are (or should be) understood, depending on the context and other factors*"[389]. This assessment may require a more or less extended and detailed analysis, depending on the situation (and the obviousness or uncertainty of the compatibility or incompatibility) [390].

The Article 29 Data Protection Working Party developed four key factors to be used during the compatibility assessment[391]: These key factors have been taken up in the new General Data Protection Regulation[392] which renders a compatibility test mandatory where "*the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law*"[393].

- **The relationship between the purposes for which the data have been collected and the purposes of further processing:** the issue is to analyse the "substance" of this relationship, to notably determine if the further processing was "*already more or less implied in the initial purposes, or assumed as a logical next step in the processing according to those purpose*s", or if there is only a "*partial or even non-existent link with the original purposes*"[394].

---

[385] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.2, p.18.

[386] *Ibid*

[387] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p.21 *et seq*. See notably p. 21: "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility*".

[388] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216), 10 April 2014, 2.2.1, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 21 May 2014).

[389] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21 *et seq*.

[390] *Ibid*.

[391] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p.23 *et seq*.

[392] The GDPR lists 5 principles but two of them are handled under the same one by the Article 29 Data Protection Working Party.

[393] Article 6 (4) of the GDPR.

[394] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, pp.23-24.

- **The context in which the data have been collected and the reasonable expectations of the data subjects as to their further use:** this criteria of reasonable expectations of privacy, which is a requirement that ensures proportionality[395] and which is a prerequisite for predictability (principle which has been highlighted by the Article 29 Data Protection Working Party[396]), has to be assessed taking into account the context of the processing, particularly the relationships between the data controller and the data subject and the expected practices in the given relationships and the related context. "*In general, the more unexpected or surprising the further use is, the more likely it is that it would be considered incompatible*"[397].

  The question of the freedom of choice of the data subject to provide data is also to consider, for example if this data subject can easily change provider or if his or her consent has been really freely given[398]. On this issue, it seems important to recall that even if individuals are totally free to publish or not publish information on social networks, the use of social networks are "*human rights enablers and catalysts for democracy*"[399], and this use may be protected for this reason on the basis of the freedom of communication[400], and on the basis of the freedom of private life[401], particularly when the social network in question becomes inevitable to remain in contact with one's contemporaries. The re-use of the data published on such networks for a purpose other than the one for which they were originally published

[395] See *supra* Section 4.1.3, under "proportionality of the very behaviour which is being restricted", in relation with the data subject's expectation of privacy.

[396] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., II.3, pp.13-14: *"further processing cannot be considered predictable if it is not sufficiently related to the original purpose and does not meet the reasonable expectations of the data subjects at the time of collection, based on the context of the collection*". Predictability " *brings legal certainty to the data subjects*" (who will "*know what to expect*", and who will be enabled to "*exercise their rights in the most effective way*"), "*and also to those processing personal data on behalf of the data controller*".

[397] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p.24.

[398] *Ibid.*

[399] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 April 2012, §15, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec(2012)4_En_Social%20networking%20services.pdf (last accessed on 21 April 2014).

[400] In this regard see for example CUEJ, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §28, available at http://curia.europa.eu/juris/liste.jsf?language=fr&td=ALL&num=C-293/12 (last accessed on 29 April 2014): the Court considers that the retention of data related to certain means of communication might have an effect on the use of such means and, consequently, on the exercise by the data subjects of their freedom of expression.

[401] The choice to exercise one's freedom of expression may be considered as a freedom of private life (see *supra*, Section 4.1.2). Moreover, Certain legal authors consider social networks as implying "*a universal right that cannot be reduced to the freedom of media, but which is a freedom of life, the right to introduce oneself to the others human being and to talk to them*" (translated from French): Assemblée nationale, rapport d'information sur les droits de l'individu dans la révolution numérique, 22 juin 2011, http://www.assemblee-nationale.fr/13/rap-info/i3560.asp. Such a "freedom of life" is actually a freedom of private life, as highlighted by the E. Court H. R.: "*Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings*": ECtHR, ch., 16 December 1992, *Niemietz v. Germany*, appl. n°13710/88, §29, http://hudoc.echr.coe.int/eng?i=001-57887 (last accessed on 12 May 2017).

may therefore be considered as incompatible (in addition to as unfair[402]). This re-use may also be considered as unexpected, since the technologies used to analyse data allow to process, to create and to link information at a level which is not commonly known by the general public.

- **The nature of the data and the impact of the further processing on the data subjects:** this criteria leads to assess the data sensitivity[403], "*the way in which the data will be further processed*" (if they will be processed by another controller, if they will be "*made accessible to a large number of persons*", if they will lead to take decisions that may impact individuals…), and the impact of the further processing on individuals, including emotional impacts (extent of the positive and the negative impact, and potential uncertainty of this impact). The more sensitive the information involved and the more negative or uncertain the impact will be, the more unlikely the further processing is to be considered as compatible use. Alternative methods allowing the controller to achieve its aim with less negative or uncertain impact on individuals[404] may be discussed during this assessment[405].
- **The safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects:** a certain number of safeguards may be put in place to compensate the weaknesses identified during the three first steps of the compatibility assessment, in order to prevent the processing to be unfair and "*any undue impact on the data subjects*"[406]. These safeguards may consist in technical and/or organisational safeguards ensuring notably "functional separation" (such as "*full or partial anonymisation, pseudonymisation, and aggregation of data*", in other words measures ensuring that the "*data cannot be used to take decisions or other actions with respect to individuals*"[407]), but also transparency (including purpose re-specification) and data subjects' control (collection of users' new consent, opt-out possibilities, data subjects' rights…)[408].

  According to the Article 29 Data Protection Working Party, functional separation, in addition to ensuring security and confidentiality, is particularly important in a big data context, when the processing does not aim at identifying people but only at detecting "*trends and correlations in the information*", and "*the extent to which this may be achieved could be an important factor in deciding whether further use of the data (…) can be considered compatible*"[409]. When the data controller is interesting in individuals,

[402] See below, "data quality".

[403] See below, "special categories of data".

[404] Which is a proportionality requirement according to the ECtHR, see above n° 4.1.3.

[405] On the entire paragraph and for quotations, see Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, III.2.2, pp.25-26.

[406] On the entire paragraph and for quotations, see Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p.26.

[407] On the entire paragraph and for quotations, see Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p.27.

[408] On the entire paragraph and for quotations, see Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p.27.

[409] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annexe 2, p.46.

and that **the processing may lead to take "measures or decisions" with regards to data subjects**, the compatibility of further use implies *"almost always" the collection of an "informed and unambiguous "opt-in" consent", in addition to* give the data subjects access to their profile and "*to the logic of the decision-making (algorithm) that led to the development of the profile*"[410]. **Such a disclosure of the "*decisional criteria*" is considered by the Working Party as a "*crucial safeguard*" in the big data area, along with the disclosure of the "*source of the data* that led to the creation of the profile**"[411].

In the context of processing for police purposes, ensuring such a transparency and collection of data subjects' consent may be counterproductive, since it may "*jeopardise*" the efficacy of a "*system designed to protect national security*" or prevent crime[412]. However (if the proposed measure complies with the other privacy and data protection requirements), alternative measures ensuring necessity and proportionality must in this case be implemented, such as limiting to the utmost extent the scope of the measure[413], as placing caveats on access and use of data[414] (including an independent control of the application of the measure), as requiring an objective and independent decision before deploying the measure[415], and as reducing the secrecy of the processing to what is strictly needed to not jeopardise the purpose of the measure[416].

4.2.3.3.2.3 Compatible use for scientific purposes

With regards to the principle of compatible use, an important question, within the framework of the MANDOLA Project, is to know if further processing for scientific purposes might be allowed.

According to Directive 95/46/EC, further processing for "*historical, statistical or scientific purposes*" must not be considered as incompatible with the original purposes, "*provided that Member States provide appropriate safeguards*"[417].[418]

---

[410] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annexe 2, p.47.

[411] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annexe 2, p.46.

[412] ECtHR, case of *Segerstedt-Wiberg and others v. Sweden*, 6 June 2006, appl. n° 62332/00, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (last accessed on 7 February 2014).

[413] Article 29 Data protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26 p. 10, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

[414] *Ibid.*

[415] *Ibid.*

[416] See for instance ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §41, http://hudoc.echr.coe.int/eng?i=001-57533; ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, http://hudoc.echr.coe.int/eng?i=001-60696, related to covert surveillance by public authorities; ECtHR, 4th Sect., 1st July 2008, *Liberty and others v. The United Kingdom*, appl. n° 58243/00, § 68-69, http://hudoc.echr.coe.int/eng?i=001-87207 (URLs last accessed on 12 May 2017).

[417] Article 6, b. of the Directive.

[418] Instruments applicable to processing for police purpose do not mention the possibility to further process data for historical, statistical or scientific purposes, at the exception of the Council Framework Decision 2008/977/JHA (Recital 6 and article 3.2, which allows such processing if appropriate safeguards are in place, such as making the data anonymous). However, according to the Article 29 Data Protection Working Party,

The Article 29 Data Protection Working Party clarified that the provision of Directive 95/46/EC is "*not intended as a general authorisation to further process data in all cases*" for such purposes, but only means that such a further processing is authorised if it complies with the other requirements of the Directive (even if these other requirements may be less rigorous for this kind of processing operations), including the requirement to be based on one of the grounds listed in Article 7[419]. Further processing for scientific purposes must also be accompanied by appropriate safeguards, to be determined during a compatibility test[420]. Relevant safeguards "*may include, among other things, full or partial anonymisation, pseudonymisation, or aggregation of the data, privacy enhancing technologies, as well as other measures to ensure*"[421] that "*the data will not be used to support measures or decisions* (taken by anyone) *regarding any particular individuals*"[422] (functional separation)[423].

On the same line, the new General Data Protection Regulation states that "*further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall (...) not be considered to be incompatible with the initial purposes*", but must respect a list of safeguards listed in article 89 of the Regulation. According to this latter article, these safeguards must be "*appropriate (...), in accordance with this Regulation*", which means that the opinion of the Article 29 Data Protection Working Party is still applicable[424]. These safeguards must moreover ensure "*that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner".* For the rest, article 89 of the Regulation authorises Member States to provide for derogations from some of the rights referred to in this Regulation, subject to appropriate safeguards in accordance with the GDPR's provisions and "*in so far as such rights are likely to render impossible or seriously*

---

such a purpose may always be accepted as soon as it stays compatible with the purposes for which data were collected: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, II.2.2, p.13, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed on 12 May 2017). On the same line, the new Police Directive states that "*processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects*".

[419] See below, our point n°6 (Data subject's consent or other appropriate legal ground).

[420] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, *op. cit.*, III.2.3, p.28.

[421] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.2, p.27.

[422] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.3, p.28.

[423] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.2, p.27.

[424] In the previous version of the GDPR, before its adoption, it was not the case. See on this issue Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit.; Estelle De Marco, Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.2.3 (on https://www.epoolice.eu/).

impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes".

Conclusion on the principle of legitimate, explicit, specified purpose and compatible use:

The principles of specified, explicit and legitimate purposes and of compatible use must be respected by the MANDOLA consortium during the course of its research, as well as by other entities or LEAs who would operate personal data processing as a result of the use of the MANDOLA outcomes.

The assessment of the MANDOLA research and of the MANDOLA outcomes have to take into account the meaning of the four following criteria (in compliance with the current and the future EU legal framework):

- **Legitimacy:** the purposes must be in accordance with the law in the broadest sense.
- **Specification:** the purposes must be sufficiently defined prior the time of the data collection, and this specification should allow identifying the processing operations that are and are not included in this specification.
- **Explicit:** the purposes must be formulated in a way that is understandable by anyone, to ensure their predictability for the data subject; the information has to be consistent and accessible.
- **Compatible use:** any other processing must not be incompatible with this first processing, whether or not it has the same purpose.

  In order to assess the compatibility, it is recommended:

  (1) To identify both the new and the original purpose;

  (2) To identify the "substance" of the relationship between these two purposes to determine if the first was already implied in the second one;

  (3) To appreciate the reasonable expectations of privacy of the data subject in the specific context, including with regard to his or her freedom of choice to give his or her data;

  (4) To assess the data sensitivity and the impact of the further processing on individuals, including emotional impacts; and

  (5) To identify the safeguards that are suitable to compensate the weaknesses identified during the previous tests and prevent any undue impact on the data subjects. Some of these safeguards may consist in technical and organisational measures ensuring functional separation, particularly important in a big data context (measures ensuring that the data cannot be used to take decisions or other measures against particular individuals, such as full or partial anonymisation, pseudonymisation, and aggregation of data), transparency (especially of the data sources and of the decisional criteria that led to the development of a profile) and data subject's consent and control.

  In the context of processing for police purposes, transparency and data subjects' consent may be replaced by alternative measures ensuring the necessity and the proportionality of the processing operations, to not jeopardise the efficacy of the system. These measures may consist in limiting to the utmost extent the scope of

the measure, in placing caveats on access and use of data (including an independent control of the application of the measure), in requiring an objective and independent decision before deploying the measure, and in reducing the secrecy of the processing to what is strictly needed to not jeopardise the purpose of the measure.

Further processing by MANDOLA partners for scientific purposes is considered compatible, if the other requirements of the EU Directive 95/46/EC are respected, and if appropriate safeguards are implemented. These safeguards have to be determined through a compatibility test as described above, in addition to the safeguards provided for in the national legislation of the data controller. This conclusion will not be different when the new General Data Protection Regulation will be applicable. However, the latter legal instrument clarifies that the safeguards must ensure "*that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*". In addition, the GDPR authorises States to legally provide for derogations from some listed other rights mentioned in the Regulation, subject to appropriate safeguards in accordance with the GDPR's provisions and "*in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*".

4.2.3.3.3 - Data quality

According to Directive 95/46/EC, to the Data Protection Convention and to the new proposed EU Regulation and Directive[425], **data must be processed fairly and lawfully, and they must be accurate and kept up to date**. Directive 95/46/EC adds that "*every reasonable step must be taken to ensure that data which are inaccurate or incomplete - having regard to the purpose for which they were collected or for which they are further processed - are erased or rectified*". The GDPR includes the same principles. It adds that data must be processed in a transparent manner in relation to the data subject (principle of transparency), but this particular principle is an extension of the principle of data subject information, targeting the way the information must be transmitted and its intrinsic quality[426].

In addition to the Data Protection Convention and the proposed new Directive which respectively is and should be applicable to processing for police purposes, the Council Framework Decision 2008/977/JHA[427] includes the principles of lawfulness, accuracy and data up-to-dateness. The principles of lawfulness and accuracy are also shared by

[425] Article 6 (a), (c), (d) of Directive 95/46/EC, art. 5 of the Data Protection Convention; art. 5 of the proposed new Regulation; art. 4 of the proposed new Directive.

[426] See recital n°58 of the GDPR.

[427] Article 4.1 of the Council Framework Decision: personal data "*shall be rectified if inaccurate and, where this is possible and necessary, completed or updated*"; article 3.1.

Recommendation 87(15) of the Council of Europe Committee of Ministers[428]. Moreover, these two latter texts add certain clarifications:

- The Council framework decision adds that "*all reasonable steps*" must be taken to ensure that data "*which are inaccurate, incomplete or not up to date are not (…) made available*", and as far as possible, *"**available information shall be added which enable the receiving Member State to assess the degree of accuracy, completeness up-to-dateness and reliability***"[429]. If it occurs that incorrect data have been transmitted or that some data have been unlawfully transmitted, the recipient must be notified and the data must be **erased or blocked**, both without delay[430].
- Rec 87 (15) states that "*as far as possible, **the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability** and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments*"[431]. In addition, "*where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data*"[432].

  Indeed, this principle of data separation ensures the fairness of the processing and the accuracy of data.

The new Police Directive provides for its part the same requirements as the GDPR, at the exception of the principle of transparency. In addition, three specific provisions impose to distinguish between data subjects, to distinguish between personal data and to not to make available inaccurate data.

- Article 6) requires - "*where applicable and as far as possible*", "*to make a clear distinction between personal data of different categories of data subjects*, such as *(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b)".*
- Article 7 requires distinguishing, as far as possible, personal data based on facts from personal data based on personal assessments.
- Article 7 requires that competent authorities *"take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available".* They must inter alia, "*as far as practicable, verify the*

[428] Appendix to Recommendation R (87) 15, Principle 3.1.

[429] Article 8 of the Council Framework Decision.

[430] Article 8 of the Council Framework Decision.

[431] Principle 3.2.

[432] Principle 3.3.

quality of personal data before they are transmitted or made available", and notify the recipient without delay "*if it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted*" (and in such a case "*the personal data shall be rectified or erased or processing shall be restricted"*). In addition, and "*as far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date"* must be added.

Conclusion on the principle of data quality:

The principles of **fairness, lawfulness, accuracy, up to dateness and transparency are applicable to personal data processing operated by the MANDOLA consortium and to personal data processing that would be operated by other natural or legal persons (other than competent authorities acting in crime prevention or repression) as a result of the use of the MANDOLA outcomes.**

These principles are also applicable to personal data processing that would be operated by LEAs, as a result of the use of the MANDOLA outcomes (the principle of fair processing is explicitly mentioned in the Data Protection Convention and the new Police Directive[433]; the principle of transparency is not explicitly mentioned in the new Police Directive and might be applied in more relative manner but is still applicable according to the principles of legal basis, of proportionality and of data subject information). These principles imply among other (1) **to distinguish between personal data of different categories of data subjects** (potential perpetrators, convicted of a criminal offence, victims, other parties); (2) to **distinguish data in accordance with their degree of accuracy or reliability** (and in particular to distinguish data based on facts from data based on opinions or personal assessments); (3) **to add to data available information on the degree of accuracy, completeness, up-to-dateness and reliability**, to be used by the recipient in case of data transmission[434]; and (4) to notify the recipient of any incorrect or unlawful transmission (in such case, data must be rectified or erased or processing must be restricted).

4.2.3.3.4 - Data minimisation

According to Directive 95/46/EC, data must be **adequate, relevant and not excessive** in relation to the purposes for which they are processed[435]. The Data Protection Convention uses the same wording as Directive 95/46/EC in relation to data that are stored. The new

[433] Compliance of data processing with the new Police Directive should be anticipated. Moreover, it has to be noted that the fairness of evidence collection may be decisive within the framework of criminal proceedings, which also argues for the application of this principle even where the current legislation does not provide explicitly for it.

[434] Literally this information should only be added to data in case of data transmission. However, ensuring data protection by design should imply to include this information at soon as possible, and to make sure it is regularly updated where appropriate.

[435] Article 6 (a), (c), (d) of Directive 95/46/EC.

General Data Protection Regulation includes the same principle, but replaces "*not excessive*" by "*what is necessary*"[436].

Regarding texts specifically dedicated to police activities, the Council Framework Decision 2008/977/JHA and the new Directive on the processing of personal data for the purpose of crime prevention[437] use the same formula as Directive 95/46/EC. Recommendation R. (87)15 of the Council of Europe do not mention the principles of adequacy and relevancy, but develops that "*the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence*"[438], and that "*as far as possible, the storage of personal data for police purposes should be limited to (…) such data as are necessary to allow police bodies to perform their lawful tasks (…)*"[439]. This approach has been preserved in the new Police Directive, according to which Member States must "*provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1)[440] and that it is based on Union or Member State law*"[441].

Conclusion on the principle of data minimisation:

Under both the current and the future legislation:

The MANDOLA consortium, during the course of its research, as well as any other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, **will have to ensure that personal data that are processed are adequate, relevant and not excessive** in relation to the purposes of the processing. The formula "*not excessive*" should be understood in accordance with the formula of the proposed new Regulation, as meaning "*limited to the minimum necessary in relation to the purposes*" for which the data are processed, since it is also a requirement of the E. Court. H. R. to ensure proportionality[442].

LEAs who would process personal data as a result of the use of the MANDOLA outcomes, **will have to respect the same principles** and, inter alia, the storage of data should be limited to the extent that data are required to allow police bodies to perform their lawful tasks. In addition, if no specific law authorises the data processing operations, they will have to

[436] Article 5c of the proposed new Directive.

[437] Article 4c of the proposed new Directive.

[438] Appendix to Recommendation R (87) 15, Principle, principle 2.1.

[439] Appendix to Recommendation R (87) 15, Principle, principle 3.1.

[440] As a reminder, Article 1(1) refers to "*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*".

[441] Article 8 of the new Police Directive.

[442] See above, Section 4.1.3. See also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, Part V, n°5.6, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf (last accessed on 12 May 2017).

ensure that the data collection will be limited to the prevention of a real danger or to the suppression of a specific criminal offence[443].

4.2.3.3.5 - Time limitation

According to Directive 95/46/EC, data must be "***kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the data are processed***"[444]. The Data Protection Convention uses a very close wording in relation to data that are stored. The new Regulation contains the same requirement, and its recital n° 39 advises controllers to establish "*time limits for erasure or for a periodic review*".

Regarding personal data processing for police purposes, the Council Framework Decision 2008/977/JHA, Recommendation 87(15) of the Council of Europe Committee of Ministers and the new Police Directive contain the same principle, even if the terms used in the first two instruments are different:

- **The Council Framework Decision states that personal data "*shall be erased or made anonymous when they are no longer required***" for the purposes for which they were or are lawfully processed[445].

  Personal data shall alternatively be "*blocked instead of erased if there are reasonable grounds to believe that erasure could affect the legitimate interest of the data subject*". In that case, blocked data may only be processed "*for the purpose which prevented their erasure*"[446].

  In addition, "*appropriate time limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data*", and "*procedural measures shall ensure that these time limits are observed*"[447]. The transmitting authority may indicate time limits for the retention of data, which must be respected by the receiving authority, unless when the data are required for a "*current investigation, prosecution of criminal offences or enforcement of criminal penalties*"[448].

- **Recommendation R. (87)15 of the Council of Europe Committee of Ministers states that "*measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary* for the purposes for which they were stored**"**.

  The Recommendation adds that for this purpose, "*consideration shall in particular be given to the following criteria: the need to retain data in the light of the*

[443] See above Section 4.2.3.3.1.

[444] Article 6, e of the Directive.

[445] By way of exception, these data may be archived "*in a separate data set for an appropriate period in accordance with national law*".

[446] Article 4 of the Council Framework Decision.

[447] Article 5 of the Council Framework Decision.

[448] Article 9 of the Council Framework Decision.

conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data"[449].

The Recommendation also contains the principle of establishment of time limits, and of periodic review: principle 7.2 states that "*rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law*".

- **The new Police Directive takes up the principle contained in Directive 95/46/EC and in the GDPR[450].** In addition, a separate article[451] addresses the issue of time limits of storage and review: Member States must "*provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data*", and "*procedural measures shall ensure that those time limits are observed*".

Regarding specifically personal data processing for scientific purposes, Directive 95/46/CE enables the storage of personal data for longer periods for historical, statistical or scientific use, provided that Member States lay down appropriate safeguards[452]. This principle is taken up by the new General Data Protection Regulation, subject to the respect of Article 89(1) of the GDPR[453] and to the implementation of appropriate technical and organisational measures.

Conclusion on the principle of time limitation:

Personal data processing operated by the MANDOLA consortium

Personal data processing that would be operated by LEAs, as a result of the use of the MANDOLA outcomes,

Under the current and the future legal framework,

Personal data processed during the course of the MANDOLA research must be kept for no longer than is necessary for the purposes of this research, and should therefore be supressed at the end of the project at the latest. National laws of the data controllers may provide for additional safeguards when the data originally processed for other purposes than research (which is the case of data available on Internet public areas) are retained

[449] Appendix to Recommendation R (87) 15, Principle 7.1.

[450] Article 4.

[451] Article 5.

[452] Article 6 (e) of Directive 95/46/EC.

[453] According to article 89(1) "*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*."

for a longer period for the purpose of research.

Personal data processing that would be operated by LEAs or by other natural or legal persons (other than competent authorities acting in crime prevention or repression), as a result of the use of the MANDOLA outcomes, must observe the same principle. In addition, time limits and periodic reviews must be established (especially by LEAs) to ensure a respect of this principle over time.

4.2.3.3.6 - Data subject's consent or other appropriate legal ground

According to Directive 95/46/EC, the data subject must have unambiguously given his or her consent to the personal data processing, unless another legal ground listed in article 7 may be used to legitimise the processing operation. These other legal grounds include (i) "*the compliance with a legal obligation to which the controller is subject*" (art. 7, c), (ii) *the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (...)*" (art. 7, e), and (iii) "*the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject*" (art. 7, f). The GDPR does not bring modifications to this principle, but tends to enhance some data subjects' rights. Particularly, it enables Member States to provide for more specific requirements and other measures to ensure lawful and fair processing in relation to the legal grounds (c) and (e) (which are the same as the legal grounds (c) and (e) contained in article 7 of the Directive 95/46/EC).

To be noted that according to Directive 95/46/EC and to the GDPR, when the processing operations are based on another legal ground than the data subject's consent, these processing operations must be "necessary" to fulfil the purpose mentioned in this legal ground.

This term should be understood as having the same meaning of the formula "*necessary in a democratic country*" of the ECHR, which includes the principles of necessity and proportionality as we have analysed it previously[454], and of the term "necessary" used in article 52, 1 of the EUCFR.[455] In this regard, as it has been highlighted by the Article 29 Data Protection Working Party, "*the term 'necessary' in the Directive provides an important safeguard in relation to legitimacy of processing of personal data*"[456].

Therefore, the data controller must **determine whether the processing operations are "necessary"** to pursue the processing purposes, by conducting a necessary and proportionality test as described in Section 4.1.3 of the current study, which firstly implies to assess whether "*there are other less invasive means to reach the identified purpose*"[457].

[454] See Section 4.1.3.

[455] See the introduction of the current Section 4.2.3.3.

[456] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 4.2.

[457] Article 29 Data Protection Working Party's Opinion 06/2014, *op. cit*., Annex 1 p. 55 (see also n°II.3, p. 11 and III.3.1, p. 29).

Data subject's consent and the legitimate interest of the controller need a particular focus, in addition to rules applicable to LEAs, which might be different.

Data subject's consent

Regarding the notion of consent, the Article 29 Data Protection Working Party has recalled that it must be a clear indication of a wish, freely given, and specific (referring "*clearly and precisely to the scope and consequences of the data processing*")[458]. Moreover, "*a fully valid consent does not relieve the data controller of his obligations, and it does not legitimise processing that would otherwise be unfair according to Article 6 of the Directive*"[459] (which includes the above mentioned principles of data quality, legitimate purpose, data minimisation, and of limitation in time).

The collection of the data subject's consent is, in certain cases, an obligation. It is for instance imperative (i) for processing traffic data for marketing purposes or added value services[460], (ii) for using location data[461], (iii) for sending direct marketing communications[462], (iv) for sending any cookie[463], and (v) for collecting sensitive data unless they are manifestly made public by the subject (or except specific obligation of the data controller or the defence of vital interests)[464].

These principles stay unchanged in the GDPR, which however clarifies that the consent of the data subject must be given in relation with each specific purpose[465]. Article 4 (11) defines the "consent" of the data subject as "*any freely given, specific, informed and*

[458] Article 2, h of Directive 95/46/EC. Article 29 data protection Working Party's Opinion 15/2011 on the definition of consent (WP187), p. 17 for the quotation, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed on 12 May 2017).

[459] Article 29 Data Protection Working Party's Opinion 15/2011 on the definition of consent (WP187), *op. cit*., p. 9.

[460] Article 6,3 of Directive 2002/58/EC, as modified by Directive 2009/136/EC.

[461] Article 9 of Directive 2002/58/EC. The definition of "consent" in Article 2(h) of Directive 95/46/EC (any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed) "*explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered*": Article 29 Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, November 2005, WP 115. p 5, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf (last accessed on 12 May 2017).

[462] Article 13 of Directive 2002/58/EC, as modified by Directive 2009/136/EC. An exception does exist for communications related to products or services that are similar to the ones already sold to the customer.

[463] Article 5, 3 of Directive 2002/58/EC as modified by Directive 2009/136/EC. The practice which consist to inform the user in the website's general terms and conditions does not meet the requirements of the Directive, even if the browser is set to reject cookies, taking into account current browsers' functionalities: Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 13, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed on 12 May 2017).

[464] Article 8 of Directive 95/46/EC. A separate opt-in consent is needed if data are collected through cookies: Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, *op. cit*..

[465] Article 6 of the GDPR refers to "one or more "specific purposes. Recital n°32 of the GDPR further clarifies that the "*consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them".*

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 7 imposes to the controller to be able to demonstrate that the data subject has consented to processing his or her personal data, and clarifies the conditions for a valid freely given consent, in relation to the way the request for consent is presented[466], to the possibility to withdraw this consent[467] and to the effect of a lack of consent on the service to be provided[468]. Article 8 clarifies that, in relation to the offer of information society services directly to a child, the consent must be given or authorised by the holder of parental responsibility over the child when the latter is under 16 years old (Member States may provide by law for a lower age for those purposes, provided that such lower age is not below 13 years).

The controller's legitimate interest

Regarding the notion of "*legitimate interest pursued by the data controller*", the Article 29 Data Protection Working Party clarifies that "*to be relevant under Article 7 (f)*", a legitimate interest must be "*lawful (i.e. in accordance with applicable EU and national law)*", must "*represent a real and present interest (i.e. not be speculative)*", and must "*be sufficiently clearly articulated"* (i.e. "*sufficiently specific*" or "*concrete*"[469]), to allow "*a balancing test to be carried out against the interest and fundamental rights of the data subject"*[470].

Such a balancing test is highly important, since its outcome "*determines whether Article 7(f) may be relied upon as a legal ground for processing*"[471]. To conduct this test, the Article 29 Data Protection Working Party advises to consider several factors by following a series of steps:

- **Assessment of the controller's legitimate interest:** "*the nature of the interests*" of the data controller must be identified (fundamental right, other personal, public or

[466] Article 7, 2 of the GDPR: "*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding*".

[467] Article 7, 3 of the GDPR: "*The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent*".

[468] Article 7, 4 of the GDPR: "*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*". Recital n°32 of the GDPR adds that "*if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*".

[469] Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*. III.3.1, p. 23 and Annex 1, p. 55.

[470] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), 9 April 2014, III.3.1, p. 25, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed on 12 May 2017).

[471] Article 29 Data Protection Working Party, Opinion 06/2014*, op. cit*. II.2, p. 9; see also III.3, p. 23.

collective interest), as well as "*the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place*"[472].

- **Assessment of the impact on the data subjects:** this step implies to identify[473]:
  - ✓ "*the nature of the data*" that will be processed;
  - ✓ the "*status of the data subject and (…) of the controller*", which means among other identifying their potential dominant position or weaknesses;
  - ✓ the way the data will be processed and the scale of the processing operations;
  - ✓ "*the fundamental rights and/or interests of the data subjects that could be impacted*";
  - ✓ *the "data subjects' reasonable expectations",* and
  - ✓ *the "impacts on the data subject",* which must be compared *"with the benefit expected from the processing by the data controller"*.
- **Establishing a provisional balance:** the outcomes of the previous step must be balanced, taking also into account the measures taken by the data controller to comply with the other requirements of the Directive.
- **Implementing additional safeguards and establishing a final balance:** a final balance between the rights and interests at stake must be established, taking into account the additional safeguards that the controller decides to implement, to reduce the weaknesses found out during the previous steps (collection of less data, short term deletion, functional separation, "*extensive use of anonymisation techniques*", "*increased transparency*", "*privacy enhancing technologies, privacy by design, privacy and data protection impact assessments*"…)[474].

  Establishing and communicating proofs of compliance: the current assessment should be documented, the documentation should be kept available to the relevant data protection authorities and its outcomes should be communicated to data subjects. However, the Article 29 Data Protection Working Party adds that the "***details of assessment and documentation*" must be adapted to the envisaged processing operations**, and to the risks they create to the rights of data subjects. This compliance test may for instance become a "*key part*" of a broader privacy impact assessment when "*a processing operation presents specific risks to the rights and freedoms of the data subjects*"[475].

This balancing test stays applicable within the framework of the GDPR, which in addition emphasises the special care to be taken where the processing involves children's personal data[476].

Rules applicable to LEAs

The principle of legitimate ground set out in Article 7 of Directive 95/6/EC is not included in the Data Protection Convention, neither in the texts applicable to processing for police

[472] Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*., Annex 1 p. 55.

[473] All quotations are coming from Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*., Annex 1 p. 55 and 56.

[474] Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*., III.3.4, p. 42, see also Annex 1 p. 56.

[475] Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*., Annex 1 p. 56.

[476] Article 6 (f) of the GDPR.

purposes. If these texts impose the collection of the data subject's consent in certain particular circumstances[477], the legal ground legitimating the processing is usually a legal basis that allows the interference, providing for appropriate and specific safeguards, and clarifying the purpose of the processing. In countries that have extended the provisions of Directive 95/46/EC to processing for police purposes, the legal ground legitimising the processing for police purposes will generally be article 7 (e), which allows processing operations that are necessary for the performance of a task carried out in the public interest (such a task being generally attributed in a legal regulation)[478]. This will stay unchanged with the new legal framework, since according to the new Police Directive, "*where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1)*"[479], The GDPR must apply to processing for such purposes, "*including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law*"[480].

This being said, the new Police Directive includes an article that deals specifically with the lawfulness of the processing. Article 8 lays down that a processing operation in the purpose of the fight against crime is "*lawful only and to the extent*" that this processing operation "*is based on Union or Member State law*", and is "necessary for *the performance of a task carried out by a competent authority for the purposes set out in Article 1(1)"*. Situations listed in this latter provision (basically crime prevention, detection and prosecution) are the legal grounds that may justify a processing operation aiming at combatting crime.

Conclusion on the principle of data subject's consent or other appropriate legal ground

The MANDOLA consortium, before processing personal data for research purposes, as well as other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, must ensure that the envisioned processing operations are legitimised by one of the legal grounds lay down in article 7 of Directive 95/46/EC and of the GDPR. If the processing operations are based on the legitimate interest of the controllers and the third parties to whom the data are disclosed (article 7f), an assessment of the processing operations legitimacy must be done taking into account the following steps, which need to be adapted to the nature of the personal data processing:

[477] For instance, according to principles 5.2 and 5.3 of the Data Protection Convention, communication of data to other public bodies than police services or to private parties are only allowed under restrictive conditions, including the situation where the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent. Article 11 of the Council Framework decision 2008/977/JHA states that "*when data are received from or made available by another Member State, they can only be further processed for a restricted list of purposes other than those for which they were transmitted. Any other purpose may only be pursued "with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law*".

[478] Article 29 Data Protection Working Party, Opinion 06/2014, *op. cit*., III.2.5, pp. 21-22.

[479] As a reminder, Article 1(1) refers to "*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*".

[480] Article 9 (2) of the Police Directive.

- Conduction of a necessity and proportionality test;
- Assessment of the lawfulness, and of the reality and concreteness of the pursued interest;
- Conduction of a balancing test between the rights at stake (including the assessment of the controller legitimate interest, the assessment of the impact of processing on the data subjects, the establishment of a provisional balance and the establishment of a final balance taking into account additional safeguards).

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to ensure that the EU law or their national law allows such processing operations, for the purposes they pursue. According to the specific provisions of this law, they may have to assess the necessity of the processing operations to fulfil their legitimate purpose (especially if the national law allowing the processing is generic). If a specific law has to be adopted to authorise the processing, it is recommended that this law takes into account the provisions of the new Police Directive (which submits to the provisions of the GDPR all the processing operations that do not pursue 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) in addition to provide for appropriate safeguards including those mentioned in the new Police Directive (which meet the requirements of the ECtHR and EUCJ).

4.2.3.3.7 - Data subject information

According to Directive 95/46/EC, the controller or his representative must provide the data subject with, at least, the identity of the controller and his potential representative, and the purpose of the processing. The Data Protection Convention contains similar provisions although they are slightly more restrictive[481]. Other information to be provided according to Directive 95/46/EC is the one that is necessary having regards to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject: it notably includes the recipient or categories of recipients of the data, and the existence of a right of access and rectification[482].

The GDPR includes the same principle, but the information to be provided is more extended. It covers inter alia the legal basis for processing, the contact details of the controller and the recipients. Where it is necessary to ensure fair and transparent processing, further information that might be required covers inter alia the period of storage, the existence of data subjects' rights and the existence of automated-decision making[483].

Such information must be given before the data subject's consent is requested, since "*data subject's consent*" is defined, in Directive 95/46/EC and in the GDPR, as a "*freely given specific and informed*" indication of his or her wishes by which this data subject

[481] Article 8a of the Convention: "*any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file*".

[482] Article 10 of Directive 95/46/EC.

[483] Article 13 of the GDPR.

signifies his or her agreement to the data processing[484]. Moreover, the Article 29 Data Protection Working Party has specified that "*the individual must be given, in a clear and understandable manner, accurate and full information of all relevant issues*"[485].

Directive 95/46/EC and the GDPR also regulate the information of the data subject where the data have not been obtained from this person. In that case, the content of the information is not highly different from the one to be provided in case of direct collection, and is still more extended in the GDPR (which notably imposes to declare "*from which source the personal data originate, and if applicable, whether it came from publicly accessible sources*", where such information is necessary to ensure fair and transparent processing). According to Directive 95/46/EC, this information must be provided "*at the time of undertaking the recording of personal data"* or no later than the time when the data are first disclosed to a third party. If this last rule is maintained in the GDPR, the new regulation authorises the information to be provided "*within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed*". The GDPR also adds that the information must be provided prior any further processing for a purpose other than that for which the personal data were obtained, and that where the personal data are to be used for communication with the data subject, the information must be provided at the latest at the time of the first communication to that data subject[486].

However, the latter provision does not apply where "*the provision of such information proves impossible or would involve a disproportionate effort*", particularly for processing for the purposes of scientific research. In this case "*Member States shall provide appropriate safeguards*"[487].Article 14, 5 (b) of the GDPR includes the same rule, subject to the conditions and safeguards referred to in Article 89(1) in relation to processing for research purposes. The GDPR moreover excludes the obligation of information in so far as it "*is likely to render impossible or seriously impair the achievement of the objectives" of the processing, but in this case the controller must "take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available*".

Finally, the GDPR regulates the way the information must be provided. Article 12 requires that the information is provided "*in a concise, transparent, intelligible and easily accessible*

[484] Article 2, h, of Directive 95/46/EC and article 4 (11) of the GDPR. In the same line, see the communication from the Commission to the European parliament, the Council, the economic and social Committee and the Committee of regions, "A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4 Nov. 2010, 2.1.5, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last accessed on 12 May 2017). See also the Article 29 Data Protection Working Party's Opinion 15/2011 on the definition of consent (WP187): "*To be valid, consent must be informed. This implies that all the necessary information must be given at the moment the consent is requested, and that it should address the substantive aspects of the processing that the consent is intended to legitimise*", p. 9; and "*there must always be information before there can be consent*", p. 19, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed on 12 May 2017).

[485] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, *op. cit*., p. 19.

[486] Article 14 of the GDPR.

[487] Article 11.2 of Directive 95/46/EC.

form, using clear and plain language, in particular for any information addressed specifically to a child". The information, which may be provided in combination with standardised icons (that the Commission might regulate in the future), must be "*provided in writing, or by other means, including, where appropriate, by electronic means*". "*When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means*". Moreover, this information must be provided free of charge (in case of excessive or unfounded request (to be demonstrated by the controller), the controller might refuse to answer or charge a reasonable fee taking into account the administrative costs of providing the information).

Regarding personal data processing for police purposes, the principle of transparency is also applicable, even if it may be restricted to not threaten the purpose of preserving national security. The reading of the ECHR requirements as interpreted by the ECtHR and of EU instruments regulating personal data processing for police purposes clearly shows that the secrecy of the processing must only be reduced to what is strictly needed to not jeopardise the efficacy of the measure, and that the extent of transparency and its limits falls within the competence of the legislator[488].

The Council Framework Decision 2008/977/JHA states that "*1. Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law*". It adds that "*2. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State*"[489].

Recommendation R. (87)15 of the Council of Europe Committee of Ministers states that "*where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced*"[490].

The new Police Directive is going farer by imposing to data controllers an obligation of information which content is close to the one included in the GDPR[491]. Member States are authorised to adopt legislative measures delaying, restricting or omitting the provision of this information, but only "*to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person*

[488] See for instance ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §41, http://hudoc.echr.coe.int/eng?i=001-57533; ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, http://hudoc.echr.coe.int/eng?i=001-60696, related to covert surveillance by public authorities; ECtHR, 4th Sect., 1st July 2008, *Liberty and others v. The United Kingdom*, appl. n° 58243/00, § 68-69, http://hudoc.echr.coe.int/eng?i=001-87207 (URLs last accessed on 12 May 2017).

[489] Article 16 of the Council Framework Decision.

[490] Appendix to Recommendation R (87) 15, Principle 2.2.

[491] Article 13 of the Police Directive.

concerned[492]*, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others*". Member States may moreover adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of these points above.

The new Police Directive also regulates the way the information must be provided. Terms are almost the same as those included in the GDPR. Main differences are that the requirement of transparency and the special protection of children are not mentioned, and that the possibility to use standardised icons is not evoked.

Conclusion on the principle of data subjects information

The MANDOLA consortium, during the course of its research, does not have to inform the data subjects on the personal data processing for the purpose of scientific research, if the provision of such information proves impossible or would involve a disproportionate effort. However, personal data controllers have to comply with specific safeguards provided for in the relevant national legislations to ensure data subjects' protection in such a situation. In addition, in order to already respect the requirements of the GDPR, which are in line with the ECHR requirements, other safeguards that are appropriate to the specific nature of the personal data processing should be implemented, including making the information publicly available.

Natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes will have to ensure the information of data subjects, unless the provision of such information proves impossible or would involve a disproportionate effort. However, in order to already respect the requirements of the GDPR, which are in line with the ECHR requirements, safeguards that are appropriate to the specific nature of the personal data processing should be implemented in order to ensure data subjects' protection, including making the information publicly available. National legislations might also provide for safeguards to implement in such case of exemption.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to make sure to implement the transparency measures provided for in the national law authorising the personal data processing. It has to be noted here that transparency is a requirement of the ECtHR, according to which secret must be reduced to what is strictly necessary to not jeopardise the efficacy of the measure. This principle is explicit in the new Police Directive, which means that a national law should not exclude transparency measures where this exclusion is not justified by the outcomes of a necessity and proportionality test, and does not pursue one of the aims listed in article 13 (3) of the Police Directive.

[492] These notion need to be understood in their meaning given by the ECtHR, and imply a necessity and a proportionality test.

4.2.3.3.8 - Data subjects' rights of access, communication, rectification and erasure

According to Directive 95/46/EC, every data subject must be guaranteed a right of access to data (which have to be communicated in "*an intelligible form*"), a right of communication, rectification, erasure or blocking of these data, and a right of "*knowledge of the logic involved in any automatic processing of data concerning him*", at least in the case of the automatic decisions described in principle 9 of the current section[493]. The right of communication covers the data, but also the existence of a personal data processing, and at least "*the purposes of the processing, the categories of data concerned, (…) the recipients or categories of recipients to whom the data are disclosed*", and "*any available information as to the source of the data*". The Personal Data Protection Convention contains similar provisions[494].

According to Directive 95/46/EC, the data subject has also the right to obtain *"notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort*"[495].

Finally, a right to object must also be provided to the data subject, at least in the situations where the data subject did not give his or her consent to the processing, and that the legal ground of the processing is the performance of a task carried out in the public interest or the legitimate interest pursued by the controller or a third party, "*save where otherwise provided by national legislation*"[496].

These principles apply to personal data processing for the solely purposes of scientific research, unless one Member State has restricted in this case the right of access, of communication, of rectification or of erasure or blocking. This may only be done by a legislative measure, "*where there is clearly no risk of breaching the privacy of the data subject"*[497].

The new General Data Protection Regulation contains the same principles and enhances data subjects' rights[498]. Inter alia, the information to be communicated in case of exercise of the right of access is extended to several elements such as "*the envisioned period for which the personal data will be stored or, if not possible, the criteria used to determine this period*", and to the "*significance and envisaged consequences of (the) processing*", in case of automated decision-making including profiling. In addition, cases in which data erasure can be obtained are more numerous, the right to object is extended to new situations, and the new Regulation introduces a right to restriction of processing and a right to data portability. Moreover, the new Regulation details the procedure to be followed where a data subject makes a request and the form the controller's answer must take[499]. The communication of

[493] Article 12 of Directive 95/46/EC.

[494] Article 8 of the Convention. The right of communication is however restricted to the existence of the processing, its main purposes, the identity and residence of the controller, and to the data subject's data "*in an intelligible form*".

[495] Article 21, c of Directive 95/46/EC.

[496] Article 14 of Directive 95/46/EC.

[497] Article 13, 2.

[498] Articles 15 to 21 of the GDPR.

[499] Article 12 of the GDPR.

any rectification or erasure to recipients to whom data have been transferred is moreover an obligation of the data controller, unless this proves impossible or involves disproportionate effort[500]. The controller must inform the data subject about those recipients if the data subject requests it.

On the opposite, in the GDPR, there is no general possible exception to data subjects' rights within the framework of personal data processing for the purpose of scientific research. However, Article 11 provides that where the purposes of the processing do no (longer) "*require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying*" with the GDPR. Moreover, in such case, where "*the controller is able to demonstrate that it is not in a position to identify the data subject*", this controller must inform the data subject accordingly and articles 15 to 20 do not apply (except where the data subject provides additional information enabling his or her identification). This principle, which is already latent in Directive 95/46/EC and therefore brings legal certainty to data controllers[501], also protects data subjects, since it does not oblige the controller to do all what is necessary to directly identify a person, when this person is only indirectly identifiable within the framework of the processing.

The rights of access, of communication, and of rectification, erasure or blocking must also be respected within the framework of personal data processing for police purposes.

- The Council Framework Decision 2008/977/JHA provides for these obligations in its articles 17 and 18. The right of communication includes "*at least*" the communication of the existence of a transmission of personal data relating to the data subject, "*information on the recipients or categories of recipients to whom the data have been disclosed*", and a communication of the data that are undergoing processing. Member States may adopt "*legislative measures*" to restrict these rights *"where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure*" to "*avoid obstructing official or legal inquiries, investigations or procedures*", to avoid prejudicing the fight against crime, to protect national or public security, or "*to protect the data subject or the rights and freedoms of others*". In this case, alternatively to the communication of the afore-mentioned elements, the national supervisory authority must "*at least*" confirm "*that all necessary verifications have taken place*". As regards the rights of rectification, of erasure and of blocking, "*Member States shall lay down whether the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority*".
- Recommendation (87) 15 of the Council of Europe Committee of Ministers develops that the public should be informed of the existence of notified police files and of its rights in

[500] Article 19 of the GDPR.

[501] Two articles of the Directive exclude the application of some requirements where such application would involve a disproportionate effort (articles 11, 2 and 12, c of the Directive). Moreover, in practice, when a request of access is received whereas the processing does not allow to know if processed data are related or not to the author of this request, the controller will generally have no other option than to answer in that sense, and will only be able to provide information details that are available (such as the purpose of the processing and the categories of data concerned).

regard to these files, by the supervisory authority[502]. "*Implementation of this principle should take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies*". Regarding data subject's rights, the latter should be granted a right of access "*in accordance with the arrangements provided for by domestic law*"[503], and a right of rectification[504]. Any data found inaccurate, excessive or irrelevant should be erased, corrected or be the subject of a corrective statement added to the file. Such corrective measure should extend as far as possible to all documents accompanying the police file and done either immediately, either at the time of subsequent processing or next communication[505]. Restrictions to the rights of access, rectification and erasure can only take place if "*indispensable for the performance of a legal task of the police or necessary for the protection of the data subject or the rights and freedoms of others*". Any refusal should be reasoned in writing, unless "*indispensable for the performance of a legal task of the police or necessary for the protection of the data subject or the rights and freedoms of others*".

- The new Police Directive provides for rules similar to those laid down in the Council Framework Decision JHA, while enhancing data subjects' rights (the text extends, inter alia, the content of the information to be provided; it regulates the form of the controller's answer to the data subject's request; it enhances the right to rectification and erasure, and it creates a right to restriction of processing).[506]

Conclusion on the principle of data subjects' rights of access, communication, rectification and erasure

MANDOLA partners or other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, must grant data subjects with a right of access, of communication, of rectification and of erasure, except where these rights are restricted by the national legislation of the controllers. A right to object must moreover be granted to data subjects. In case the personal data processing does not allow identifying directly an individual, such information will have to be provided. When the GDPR will be applicable, for processing where the controller is able to demonstrate that it is not in a position to identify the data subject, this controller will have to inform the data subject accordingly and data subject's rights will not apply, except where the data subject provides additional information enabling his or her identification.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to comply with their national legislation on data subject's right of access, communication, rectification and erasure. If a specific law has to be adopted to authorise the processing, it is recommended that this law takes into account the

[502] Appendix to Recommendation R (87) 15, Principle 6.1.

[503] Appendix to Recommendation R (87) 15, Principle 6.2.

[504] Appendix to Recommendation R (87) 15, Principle 6.3.

[505] Appendix to Recommendation R (87) 15, Principle 6.3.

[506] Articles 12 to 18 of the Police Directive.

provisions of the new Police Directive, in order to ensure compliance with the future EU framework.

4.2.3.3.9 - Prohibition of automated decision

According to Directive 95/46/EC, a person cannot "*be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him*" (such as his performance at work, creditworthiness, reliability, conduct, etc.). National law can however authorise such an automatic decision if it "*lays down measures to safeguard the data subject's legitimate interest*".[507] The Data Protection Convention does not include a similar principle, but the modernisation proposals of this Convention, adopted on 30th November 2012, state that "*any person shall be entitled (…) not to be subject to a decision significantly affecting him/her, based solely on an automatic processing of data without having their views taken into consideration*"[508].

The General Data Protection Regulation takes up the principle set out in Directive 95/46/EC, extending the prohibition to all decisions based solely on automated processing, including profiling, where such decisions produce legal effects concerning the data subject or similarly significantly affect him or her[509]. Three exceptions are the need for entering into or to perform a contract, the authorisation provided by law and the data subject's explicit consent. In all cases, suitable safeguards must be implemented, "*at least the right*" of the data subject "*to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*". Moreover, unless exception subject to suitable measures to safeguard the data subject's rights and freedoms and legitimate interests[510], such automated decisions cannot be based on special categories of personal data[511] (also called "sensitive data" and studied in the following section).

The same principle of prohibition of decisions based solely on automated processing also applies to processing for police purposes. The Council Framework Decision 2008/977/JHA does only authorise such a decision, when it produces an "*adverse legal effect for the data subject or significantly affects him*", if authorised by a law "*which also lays down measures to safeguard the data subject's legitimate interests*"[512]. Recommendation R. (87)15 of the Council of Europe Committee of Ministers does not contain such a principle, but Principle 1.2 develops that "*new technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation*".

[507] Article 15 of the Directive 95/46/EC.

[508] Article 8, a of the proposals.

[509] Article 22 of the GDPR.

[510] Where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes or where processing is necessary for reasons of substantial public interest

[511] See next section.

[512] Article 7 of the Council Framework Decision.

The new EU Police Directive takes up the principle mentioned in the Council Framework Decision and reinforces it[513]. 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*", must be "*prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller*". Such a decision must not be based on special categories of data mentioned in Article 10 of the Police Directive (also called "sensitive data") "*unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place*". Finally, "*profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law".*

Conclusion on the principle of prohibition of automated decisions

The MANDOLA consortium, during the course of its research, and other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, must ensure that any potential personal data processing will not lead to decisions which produce legal effects concerning a data subject or which significantly affect this data subject, and which would solely be based on automated processing of data intended to evaluate certain personal aspects relating to this data subject.

This principle will be reinforced when the General Data Protection Regulation will be applicable. All decisions based solely on automated processing, including profiling, producing legal effects concerning the data subject or similarly significantly affect him or her, will be prohibited, unless exception that do not seem applicable.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to comply with their national legislation in relation with automated processing of data intended to evaluate certain personal aspects relating to the data subject that may lead to decisions affecting individuals. This legislation should at least prohibit such decisions when based solely on such automated processing, unless specific safeguards are in place. If a specific law has to be adopted to authorise the processing, it is recommended that this law takes into account the provisions of the new Police Directive, in order to ensure compliance with the future EU framework (any processing of this kind must be specifically authorised by law and must "*provide appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller*"; such a decision must not be based on special categories of data mentioned in Article 10 of the Police Directive (also called "sensitive data") "*unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place*"; and "*profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law").*

[513] Article 11 of the Police Directive.

4.2.3.3.10- Enhanced protection of some sensitive data

The notion of "*sensitive data*" is not a legal one, but is generally employed in order to designate some "*special categories of data*", whose processing is regulated by article 8 of the Directive 95/46/EC, article 9 of the General Data Protection Regulation and article 10 of the Police Directive. In addition, some other data are considered more sensitive and therefore benefit from greater protection in Directive 2002/58/CE modified in 2009.

Special categories of data

According to Directive 95/46/EC, the expression "Special categories of data" covers the two following categories of data:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life[514]. The Data Protection Convention provides for a close definition[515].

  Under Directive 95/46/EC, the processing of such data is prohibited, apart from a number of exceptions exhaustively listed. Among these exceptions lies the data subject explicit consent to the processing (where the national law allows such an exception) and the situation where the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims. National laws may also provide for other exceptions for reasons of substantial public interest, if they also provide for suitable safeguards[516].

  The Article 29 Data Protection Working Party stressed that "*it would be inappropriate to conclude (…) that the fact that someone has made special categories of data manifestly public under Article 8(2)(e) would be - always and in and of itself - a sufficient condition to allow any type of data processing, without an assessment of the balance of interests and rights at stake as required in Article 7(f)*" [517], when such a legal ground applies.

- Personal data "*relating to offences, criminal convictions or security measures*"[518]. Such data "*may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority*".

[514] Article 8, 1 of Directive 95/46/EC/

[515] Ethnic origin and trade-Union membership are not included in the definition, but "other beliefs" are included in it. The processing of criminal convictions, which we will evoke below, is also included in the definition.

[516] Article 8 of Directive 95/46/EC.

[517] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), 9 April 2014, III.1.2, p. 15, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed on 12 May 2017).

[518] Article 8, 5 of Directive 95/46/EC.

The new General Data Protection Regulation adds, to the list of special categories of data, "*sexual orientation"*[519], "*genetic data", and "biometric data (processed) for the purpose of uniquely identifying a natural person".* However, data relating to criminal convictions and offences are removed from this list, and are regulated in a separate provision.

The protection offered by the new Regulation is close to the one offered by Directive 95/46/EC, but the list of the exceptions that allow processing sensitive data (excluding data relating to criminal convictions and offences) is extended. Processing special categories of data is notably possible if processing is necessary for scientific research purposes, subject to the conditions and safeguards referred to in article 89 (1) of the Regulation[520].

With the exception of personal data related to criminal offences, special categories of data are also subject to reinforced protection when they are processed by police services.

- The Council framework decision 2008/977/JHA states that special data as defined by Directive (with the exception of personal data related to criminal offences) 95/46/EC "*shall only be permitted when this is strictly necessary and when the national law provides adequate safeguards*"[521].
- Recommendation (87) 15 of the Council of Europe Committee of Ministers states that "*the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not prescribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry*"[522].
- The new Police Directive takes-up the same definition of special categories of data than the GDPR (excluding too from this category personal data related to criminal offences). Processing such data must be "*allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject*", and only in two situations (where "*authorised by Union or Member State law*", either in order "*to protect the vital interests of the data subject or of another natural person*", or "*where such processing relates to data which are manifestly made public by the data subject*").[523]

<u>Other sensitive data</u>

Sensitive data covered by directive 2002/56/EC are the following:

- **Communications and related traffic data:** "communication" means "*any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service*". "*This does not include any information conveyed as part of a broadcasting service to the public over an electronic*

[519] To be noted that "gender identity" was also a sensitive data in the draft regulation as amended by the European Parliament in March 2014, but it has disappeared from the definitive version.

[520] Article 9 of the GDPR.

[521] Article 6 of the Council Framework Decision.

[522] Principle 2.4.

[523] Article 10 of the new Police Directive.

communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information"[524]. Member States shall ensure their confidentiality and in particular shall prohibit any kind of storage, interception or surveillance by persons other than users, without the consent of the users concerned[525].

- **Traffic data:** "traffic data" means "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*"[526]. Providers of publicly available electronic communication services have the obligation to anonymise traffic data, as a principle. They only may process traffic data for the purpose of subscriber billing and interconnection payments, up to the end of the period during which the bill may lawfully be challenged or payment pursued, and for the purpose of marketing electronic communications services or for the provision of value added services, to the extent and for the duration necessary for such services or marketing, if the user to whom the data relate has given his informed[527] consent. This user shall moreover be given the possibility to withdraw his consent at any time[528].
- **Location data other than traffic data:** "location data" means "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*"[529]. Location data other than traffic data may only be processed when they are made anonymous or with the informed consent of the concerned user, *"to the extent and for the duration necessary for the provision of a value added service*". The information to be provided to the user is related to the type of data that will be processed, to the purposes and duration of the processing and to whether the data will be transmitted to a third party for the purpose of providing the value added service. Users must be given the possibility to withdraw their consent at any time, or, using a simple means and free of charge, to temporarily refusing the processing of their location data for each connection to the network or for each transmission of a communication[530].

Despite these latter sensitive data seem literally to be protected only against electronic communications operators and Internet access provider[531], they are in practice protected

[524] Article 2 of Directive 2002/58/EC.

[525] Article 5 of Directive 2002/58/EC.

[526] Article 2 of Directive 2002/58/EC.

[527] The user must receive information on the types of traffic data which are processed and of the duration of such processing.

[528] Article 6 of Directive 2002/58/EC.

[529] Article 2 of Directive 2002/58/EC.

[530] Article 9 of Directive 2002/58/EC.

[531] As we analysed it at the beginning of this section related to the EU legislation, article 3 of the Directive states that this latter text applies only within the framework of the provision of electronic communications services, which relates to the services operated by electronic communications operators and Internet access provider. The Article 29 Data Protection Working Party relies itself on the letter of this article 3, and considers that the provisions of the Directive concerning the processing of geolocalisation data do only apply to electronic communications operators (Article 29 Data Protection Working Party, Opinion 13/2011 on

against any stakeholder. Indeed, the spirit of the Directive and a part of its letter impose to the other stakeholders to respect the confidentiality of communications and traffic data, and impose to value added service providers to respect the confidentiality of location data[532]. In addition, communications, traffic data and location data remain strongly protected on the basis of Directive 95/46/EC and the ECHR[533].

Communications, traffic data and location data also benefit from an enhanced protection when they are collected for police purposes. Exceptions to the protection granted to these data are possible when legally authorised for one of the grounds listed in the Directive (State security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system), if this authorisation "*constitutes a necessary, appropriate and proportionate measure within a democratic society*", which means inter alia that the measure shall only authorise the retention of data for a limited period of time[534] [535].

Geolocation services on smart mobile devices (WP 185), 16 May 2011, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf -last accessed on 12 May 2017).

[532] See especially articles, 5 (1), 5 (3), 9 and 13 of the Directive, and recitals n° 1 (which refers to the "electronic communications **sector**), 2, 3, 4 (which states that the Directive aims to protect privacy "regardless of the technologies used"), 5, 21, and 35. For further details of this analysis, see Estelle De Marco in Estelle De Marco et al., Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.2.3., point n°10, p. 69 et seq.

[533] The Article 29 Data Protection Working Party considers that, "*given the sensitivity of the processing of location data*", such processing must always be justified by the collection of the prior informed consent of the person who is concerned, for each purpose for which the data are processed, on the basis of Directive 1995/46/EC. According to the working party, such consent is indeed "*the main applicable ground for making data processing legitimate when it comes to the processing of the location of a smart mobile device in the context of information society services*" (Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185), 16 May 2011. Given the highly confidential character of other types of traffic data and of communications, as well as the protection granted by the ECtHR to privacy towards monitoring techniques (see for ex. ECtHR, 4th Sect., 3 April 2007, *Copland v. the United Kingdom*, appl. n° 62617/00, § 44, http://hudoc.echr.coe.int/eng?i=001-79996, to the secrecy of private communications in general (Ivana Roagna, " Protecting the right to respect for private and family life under the European Convention on Human Rights", Council of Europe human rights handbooks, Council of Europe, 2012, p. 32, available at: www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf; see also Commission, plen., 27 February 1995, *B.C. v. Switzerland*, appl. n°21353/93, http://hudoc.echr.coe.int/eng?i=001-2039), including when they take place in a business environment (Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 44, referring to the judgement ECtHR, ch., 16 December 1992, *Niemietz v. Germany*, appl. n°13710/88, §50, http://hudoc.echr.coe.int/eng?i=001-57887; ECtHR, ch., 25 June 1997, *Halford v. the United Kingdom*, appl. n°20605/92, §§ 44-46, http://hudoc.echr.coe.int/eng?i=001-58039, and to electronic communications more specifically, this notion being extended to the personal Internet usage (ECtHR, 4th Sect., 3 April 2007, *Copland v. the United Kingdom*, appl. n° 62617/00, § 41, http://hudoc.echr.coe.int/eng?i=001-79996, it may reasonably be concluded that the above mentioned opinion of the Article 29 Data Protection Working Party may be extended to these private life elements. Moreover, the ECHR might also be brought into play within the courts (URLs last accessed on 12 May 2017).

[534] Article 15 of Directive 2002/58/EC.

[535] The recording of communications and the related traffic data may also be legally authorised when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication: article 5 of Directive 2002/58/EC.

Directive 2006/24/EC, which regulated specifically the obligation for operators to retain some data for police needs, adds that the availability of such data must be ensured "*for the purpose of the investigation, detection and prosecution of serious crime*". However, the content of this Directive is not fully compliant with the ECHR. In 2014, the EUCJ has ruled that some of its provisions are disproportionate and therefore do not comply with the requirements for the protection of fundamental rights[536]. Beforehand and afterward, some EU Member States national Constitutional courts considered that the national texts implementing this Directive are contrary to their domestic Constitution[537], bearing in mind that the Article 29 Data Protection Working Party[538] and the European Data Protection Supervisor[539] already highlighted, in the past, that the Directive was not compliant with the ECHR. As a result, Directive 2006/24/EC is currently not binding for EU Member States, which can choose to implement it or not in their territory[540], The European Commission reserving the right to control "*existing EU data retention laws*"[541].

Conclusion on the principle of enhanced protection of sensitive data

The MANDOLA consortium, during the course of its research, must ensure that:

- It does not process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life. If such personal data, collected in Internet public spaces, are not avoidable, the consortium must take this situation into account, during the assessment of the legitimacy of the processing's legal ground which should be article 7 (f), to ensure that

[536] Judgment of the Court, 8 April 2014, joined cases C-293/12 and C-594/12 (case "Digital Rights Ireland Ltd"), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=210837 (last accessed on 12 May 2017).

[537] Regarding Germany, see for instance European Commission press release, "Data retention: Commission takes Germany to Court requesting that fines be imposed", IP/12/530, 31 May 2012, http://europa.eu/rapid/press-release_IP-12-530_en.htm. The Constitutional Court of the Republic of Slovenia also abrogated the national data retention provisions in a judgment of 13 July 2014, following the CJEU decision: see EDRI, "Slovenia: Data retention unconstitutional, deletion of data ordered", 16 July 2014, https://edri.org/slovenia-data-retention-unconstitutional/ (URLs last accessed on 12 May 2017).

[538] Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism (WP 99), 9 November 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf (last accessed on 12 May 2017).

[539] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf. See also Opinion 2005/C 298/01 on the proposal for Directive 2006/24/EC, 26 Sept. 2005, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_EN.pdf (URLs last accessed on 23 May 2017).

[540] See the European Commission statement on national data retention laws, 16 September 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm (last accessed on 12 May 2017).

[541] Diego Naranjo, "European Commission will 'monitor' existing EU data retention laws", 29 July 2015, https://edri.org/european-commission-will-monitor-existing-eu-data-retention-laws/ (last accessed on 12 May 2017).

the consortium's interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

- It does not process communications, traffic data and location data. If such data, collected in Internet's public spaces, are not avoidable, all the necessary measures to make the data anonymous as soon as possible must be implemented.

The same conclusions apply to other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to comply with their national legislation in relation with personal data processing revealing special categories of data, or concerning communications, traffic data and location data. Such legislation should only authorise such processing where it is strictly necessary, in the respect of ECHR principles (clarified in the new Police Directive), in specific cases, and provide for appropriate safeguards (including time limits and clarification of crimes that may authorise such processing; moreover, communications intercepts should call for enhanced protection). If a specific law has to be adopted to authorise the processing, it is recommended that this law takes into account the specificity of the system to be used and the source of the information, to identify the safeguards suitable to that particular system.

4.2.3.3.11 - Security and confidentiality of the processing

According to Directive 95/46/EC, "*the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*"[542]. Such measures must "*ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected*", having regards "*to the state of the art and the cost of their implementation"*[543]. When processing operations are carried out on his behalf, the controller must "*choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out",* and this controller *"must ensure compliance with those measures*"[544], on the basis of a contract stipulating amongst other that "*the processor shall act only on instructions from the controller*", and that the obligation to implement security measures are *"incumbent on the processor*". Unless law requires otherwise, "*any person acting under the authority of this controller*" (staff, processor, staff of the processor…) must not process the data "*except on instructions from the controller*"[545].

[542] Article 17 of Directive 95/46/EC.

[543] Article 17.1 of Directive 95/46/EC.

[544] Article 17.2 of Directive 95/46/EC

[545] Article 16 of Directive 95/46/EC

The data Protection Convention, in shorter terms, provide for the same principle of data security[546].

The new General Data Protection Regulation maintains the principle of data security but expands it to all kind of risks[547]. The new rule is that the controller and the processor must "*implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*", "*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*" (this sentence referring to risk management, which is also included in the privacy impact assessment to be conducted in several situations[548]). The technical and organisational measures to be implemented include, "*inter alia as appropriate*"[549], "*(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; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;* (and) *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*".

As regards risks to be taken into account "*in assessing the appropriate level of security*"[550], they are those, "*in particular*"[551], that are "*presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*" [552]. According to this formula, risks to freedoms that are not presented by processing must therefore also be taken into account.

Moreover, personal data breaches will have to be notified to the supervisory authority, and, in some situations, to the data subject[553].

The security and confidentiality requirements are also to be respected within the framework of processing for police purposes.

- The Council Framework Decision 2008/977/JHA requires the logging and documentation of all transmissions of personal data, to ensure "*proper data integrity and security*", in addition to enable the verification of the lawfulness of the data processing[554]. In addition, "*competent authorities must implement appropriate technical and*

[546] Art 7 of the Convention: "*Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination*".

[547] Article 32 of the General Data Protection Regulation.

[548] Article 35 of the General Data Protection Regulation.

[549] Article 32 of the General Data Protection Regulation.

[550] Article 32 §2 of the General Data Protection Regulation.

[551] *Ibid.*

[552] *Ibid.*

[553] Articles 33 and 34 of the General Data Protection Regulation.

[554] Article 10 of the Council Framework Decision.

organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected"[555]. These measures must be designed to ensure a list of ten actions, including inter alia equipment access control, data media control, storage control, user control, data access control and input control. Processors may be designated only if they comply with these requirements, and such processors can only process data on the basis of a written contract or a legal act[556]. Finally, persons who access the data must act on instructions of the competent authority, and must respect all applicable data protection requirements[557].

- Recommendation R. (87)15 of the Council of Europe Committee of Ministers states that *"the responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration. The different characteristics and contents of files should, for this purpose, be taken into account*"[558].

The new Police Directive enhances these security requirements. Firstly, it provides for the same ten actions contained in the Council Framework Decision 2008/977/JHA, to be ensured through the implementation of security measures. This implementation by the controller and the processor must take into account, following the same wording as in the GDPR, "*the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*"[559], particularly in case special categories of data are processed[560]. Secondly, personal data breaches must be notified to the supervisory authority[561], as well as, in certain cases, to the data subject.[562].

Conclusion on the principle of data security and confidentiality

The MANDOLA consortium, in relation with personal data processing operations taking place during the MANDOLA research, as well as other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process data as a result of the use of the MANDOLA outcomes, must implement appropriate technical

[555] Article 22 of the Council Framework Decision.

[556] Article 22 of the Council Framework Decision.

[557] Article 21 of the Council Framework Decision.

[558] Appendix to Recommendation R (87) 15, Principle 8.

[559] Article 29 of the new Data Protection Directive.

[560] *Ibid.*

[561] Article 30 of the new Data Protection Directive.

[562] Article 31 of the new Data Protection Directive.

and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. The level of security must be appropriate to the risk presented by the processing and the nature of processed data, and the consortium must ensure that any processor fulfils this obligation.

The General Data Protection Regulation will enhance this obligation, by imposing in practice the performance of a risk analysis, by extending the risk analysis to all the risks to freedoms due to processing operations and not only to the risks posed by this processing, and by listing some imperative measures to be taken. Moreover, personal data breaches will have to be notified to the data protection authorities, and in certain cases to the data subjects.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will also have to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in compliance with their national legislation. The level of security should be appropriate to the risk presented by the processing and the nature of processed data, and the measures to implement should be designed to ensure a list of ten actions, including inter alia equipment access control, data media control, storage control, user control, data access control and input control. Processors may be designated only if they comply with these requirements, may only process data on the basis of a written contract or a legal act, and persons who access the data must act on instructions of the competent authority, and must respect all applicable data protection requirements.

If a specific law has to be adopted to authorise the processing, it is recommended that this law takes into account the provisions of the new Police Directive, to ensure compliance with the future EU framework, which is in line with ECHR and EUCFR requirements. In this regard a risk assessment must in practice be conducted, special scrutiny must surround the processing of special categories of data, and personal data breaches must be notified to the supervisory authority, as well as, in certain cases, to the data subject.

4.2.3.3.12 - Data protection authority supervision

According to Directive 95/46/EC, Member States must "*provide that one or more (independent) public authorities are responsible for monitoring the application*", within their territory, of their national provisions implementing the Directive. Inter alia, these authorities must have powers of investigation and effective powers of intervention, "*the power to engage in legal proceedings where the national provisions (…) have been violated or to bring these violations to the attention of the judicial authorities",* and the power to issue decisions[563].

The Data Protection Convention does not include this principle, but the consolidated proposal for modernisation of this Convention provides for provisions that are very similar to

[563] Article 28 of Directive 95/46/EC.

those of Directive 95/46/EC, taking also some inspiration from the new General Data Protection Regulation[564].

In addition, according to Directive 95/46/EC, the personal data controller must notify the national supervisory authority "*before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes*". Member States may provide for the simplification of or exemption from notification in some cases and under some conditions that are exhaustively listed in the Directive.[565]

The new General Data Protection Regulation includes the same principle of establishment of independent authorities in charge of ensuring compliance with the data protection legislation, giving more details on these authorities' powers of investigation and intervention[566]. However, the principle of systematic notification disappears.

Instead, the controller and processor must designate a data protection officer in certain situations (where "*the processing is carried out by a public authority or body, except for courts acting in their judicial capacity*"; where "*the core activities (...) consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale*"; or where "*the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10*") [567].

In addition, the controller must "*consult the supervisory authority prior to processing*" where the data protection impact assessment he must perform in certain situations[568] "*indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk*".

For the rest, such as in the current applicable legislation, codes of conducts and their monitoring[569], as well as certification[570], are encouraged, and the data protection authority has *inter alia* the duty to "*monitor and enforce*" the application of the Regulation and to "*handle complaints*" lodged by data subjects[571]. The Regulation moreover provides for

---

[564] Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, September 2016, https://www.coe.int/en/web/data-protection/modernisation-convention108 (last accessed on 23 May 2017). The proposal requires that each party provides "*for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention"; "To this end, such authorities"* must be granted with several powers including "*powers of investigation and intervention*", "*powers to issue decisions with respect to violation of the provisions of this Convention"* and to "*engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention"* (article 12 *bis* of the proposal).

[565] Article 18 of Directive 95/46/EC.

[566] Articles 51 *et seq.* of the General Data Protection Regulation.

[567] Article 37 of the General Data Protection Regulation.

[568] See *infra* our Section 4.2.3.3.13.

[569] Articles 40 and 41 of the General Data Protection Regulation.

[570] Articles 42 and 43 of the General Data Protection Regulation.

[571] Article 57 of the General Data Protection Regulation.

specific rules on co-operation between the lead data protection authority and the other data protection authority concerned where cross-border processing are the subject of a complaint or of an investigation[572].

The principle of data protection authority supervision also applies in the sector of processing for police purposes.

- The Council Framework Decision 2008/977/JHA provides for the same principles of Directive 95/46/EC in terms of establishment of independent national supervisory authorities with investigative powers and effective powers of intervention[573], and in terms of consultation of the relevant authority prior to certain categories of processing (which are processing of personal data "*which will form part of a new filing system to be created where (..) special categories of data (…) are to be processed*", or where "*the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms*" of the data subject[574]).
- Recommendation R. (87)15 of the Council of Europe Committee of Ministers states that the relevant supervisory authority should be consulted "*in advance in any case where the introduction of automatic processing methods raises questions about the application of (the) recommendation*", and that "*permanent automated files*" should all be notified to this authority. "*Ad hoc files which have been set up at the time of particular inquiries should also be notified*", either "*in accordance with the conditions settled with*" this authority ("*taking account of the specific nature of these files*"), "*or in accordance with national legislation*"[575].
- The new Police Directive reinforces the supervisory powers of national supervisory authorities, especially by extending the obligation of prior consultation to all the situations where (1) a data protection impact assessment "*indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk*", and (2) where "*the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subject*"[576]. In addition, controllers must "*designate a data protection officer*" ("*Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation*") [577].

Conclusion on the principle of data protection authority supervision

The MANDOLA partners, before processing personal data during the course of the MANDOLA research, must notify these processing to the relevant data protection authorities, and respond to any request from these authorities, in accordance with the national provisions of the controllers.

[572] Articles 56 and 60 of the General Data Protection Regulation.

[573] Article 25 of the Council Framework Decision.

[574] Article 23 of the Council Framework Decision.

[575] Appendix to Recommendation R (87) 15, Principles 1.3 and 1.4.

[576] Article 28 of the new Directive.

[577] Article 32 of the new Directive.

LEAs and other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes will also have to notify their personal data processing to their respective data protection authority, and may also have to consult this authority prior any processing, depending on the nature of the latter and their specific national provisions, and subject to the provisions of a specific legal basis that would be required in order to authorise specific processing operations.
If such a specific legal basis has to be adopted to authorise the use of the MANDOLA outcomes, it is recommended that this legal basis takes into account the provisions of the new Police Directive, in order to ensure compliance with the future EU framework (especially by imposing a prior consultation of the authority in case processing operations involve a high risk to the rights and freedoms of data subject).

4.2.3.3.13 - Liability and accountability of the data controller

According to Directive 95/46/EC, the controller has the responsibility to ensure that the personal data processing operations he carries out comply with the data protection legislation[578].

The controller is the "*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*"[579].

The capacity to "*determine*" these purposes and means is usually analysed in the light of "*factual elements or circumstances of the case*"[580]. The controller is therefore the person who determines in practice the purposes and means of the processing, regardless of whether the processing is or not legally compliant. The analysis must focus on factual elements[581], and in case of doubt it may be necessary to analyse the "*degree of actual control exercised by a party*"[582], and the "*level of influence on the 'why' and the 'how'*" of "*certain processing activities*"[583]. The approach is therefore pragmatic, and places "*emphasis on discretion in determining purposes and on the latitude in making decisions*"[584]. The notion of "*means*" itself includes "*both technical and organisational questions*": it does not only refer "*to the technical ways of processing personal data, but also to the 'how' of processing, which includes inter alia questions like "which data shall be processed" and "when data shall be deleted*"[585]. In situations where "*multiple actors*

[578] Article 6, 2 of Directive 95/46/EC.

[579] Article 2, d of Directive 95/46/EC.

[580] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, III, 1a, p. 10 *et seq*., available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (last accessed on 24 May 2017).

[581] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., III, 1a, p. 10.

[582] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 14.

[583] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 15.

[584] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 15.

[585] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 16.

interact in the processing of personal data"[586], these different actors may be "*joint controllers*" and may therefore share the responsibility to comply with legal obligations. Each of them may also be the unique controller for some data processing operations that remain under their control (and if the processed data are intended to be transferred to a shared infrastructure, they remain inter alia liable for ensuring that the data transfer is secured[587]). In these situations, liabilities (in terms of "*compliance with data protection rules*" and of "*responsibilities for possible breach of these rules*"[588]) must be clearly allocated, on the basis of a "*substantive and functional approach*", to not lead to a dilution of responsibilities or to "*an unworkable distribution of responsibilities*"[589]. On this issue, it is notably important to "*make clear if every controller is competent to comply with all data subject's rights or which controller is competent for each right*"[590]. In addition, the "*participation of the parties to the joint determination may take different forms and does not need to be equally shared*"[591]. In situations where different actors decide *"to set up a shared infrastructure*", even to pursue "*their own individual purposes*", these actors are joint controllers, as soon as they all determine "*the essential elements of the means to be used*", at least in this extent[592]. Finally, regarding the person who is controller within an organisation, "*preference should be given to consider as controller the company of body as such rather than a specific person within the company of the body*", "*unless there are clear elements indicating that a natural person shall be responsible*"[593].

The Directive also develops that the EU Member States must provide that "*any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive 95/46/EC is entitled to receive compensation from the controller for the damage suffered*"[594]. "*Every person*" must be granted with the right to a "*judicial remedy for any breach*" of his or her rights as guaranteed by the national law applicable to the processing[595], and Member States must impose sanctions in case of infringement of the provisions protecting personal data at the national level[596].

The Data Protection Convention contains similar provisions, even if the responsibility of the controller is not clearly mentioned[597]. The controllers' obligation to "*take all appropriate measures to comply with the obligations*" of the Convention and to "*be able to demonstrate,*

[586] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 19.

[587] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 21.

[588] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 24.

[589] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 20.

[590] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 24.

[591] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 21.

[592] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., pp. 21-22.

[593] Article 29 Data Protection Working Party, Opinion 1/2010, *op. cit*., p. 17.

[594] Article 23 of Directive 95/46/EC.

[595] Article 22 of Directive 95/46/EC.

[596] Article 24 of Directive 95/46/EC.

[597] Articles 2 and 10 of the Convention.

in particular (...), that the data processing under their control is in compliance with the provisions of" the Convention is however clearly mentioned in the proposal for modernisation of this Convention[598], which also includes some of the principles provided for in the new General Data Protection Regulation[599].

Indeed, the new General Data Protection Regulation (GDPR) contains similar principles as Directive 95/46/EC[600] but is clearer on and strengthens controllers' liability and accountability.

Liability

The GDPR develops that the data subject has the right to "*lodge a complaint with a supervisory authority*"[601], has the "*right to an effective judicial remedy against a supervisory authority*"[602], and has the "*right to an effective judicial remedy against a controller or a processor (...) before the courts of the Member State where the controller or processor has an establishment*, *(...)* (or) *where the data subject has his or her habitual residence"*[603] *(*unless in this last case "*the controller or processor is a public authority of a Member State acting in the exercise of its public powers*"[604]). The regulation also grants data subjects with a "*right to receive compensation from the controller or processor*" [605] for any damage suffered unless, in relation with damages caused by processing, where the controller has complied with his or obligations of the Regulation[606]. Each supervisory or data protection authority is also empowered with several investigative and corrective powers, including "*to carry out investigations in the form of data protection audits*", to order a controller to comply with the Regulation and "*to impose an administrative fine*"[607] under general conditions[608].

Accountability

In addition, the new Regulation imposes to the controller to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with*" the Regulation, "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood*

[598] Article 8 *bis* of the consolidated version of September 2016 (finalised on 16 June 2016).

[599] For instance the principle of privacy by design (art. 8 bis, 2).

[600] In relation with the definition of the controller and processor see Art. 4 §7 and 8, and Art. 26 of the General Data Protection Regulation.

[601] Article 77 of the General Data Protection Regulation.

[602] Article 78 of the General Data Protection Regulation.

[603] Article 79 of the General Data Protection Regulation.

[604] *Ibid.*

[605] Article 82 of the General Data Protection Regulation.

[606] *Ibid.*

[607] Article 58 of the General Data Protection Regulation.

[608] These conditions are described in Article 83 of the General Data Protection Regulation.

and severity for the rights and freedoms of natural persons"[609]. These measures might include "*appropriate data protection policies*" and "*adherence to approved codes of conducts* (...) *or approved certification mechanisms*" [610].

Moreover, the controller has the duty to "*maintain a record of processing activities under its responsibility*" [611], which must contain a number of data listed such as the *"purposes of the processing*", the categories of recipients, of data subjects, of personal data, and "where possible (...) envisaged times limits for erasure" and "a general description of the technical and organisational security measures"[612]. Each processor must itself "maintain a record of all categories of processing activities carried out on behalf of a controller", also containing some listed information[613]. To be noted that these obligations of record are not applicable to organisations "*employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data* (...)"[614].

Data protection by design and by default

The controller must also ensure "*data protection by design and by default*" [615], which means that he or her must, "*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*"[616]. This must be done "*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*"[617]. Data protection by design and by default also means that the controller must "*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*"[618]. An "*approved certification*

[609] Article 24, 1 of the General Data Protection Regulation. Article 5 relating to "principles relating to processing of personal data" also mentions in its §2 this principle of accountability: "*the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".

[610] Article 24, 2 and 3 of the General Data Protection Regulation.

[611] Article 30 §1 of the General Data Protection Regulation.

[612] *Ibid.,* §1.

[613] *Ibid.,* §2.

[614] *Ibid.,* §3.

[615] Article 25 of the General Data Protection Regulation.

[616] *Ibid.,* §1.

[617] *Ibid.,* §1.

[618] *Ibid.,* §2.

mechanism (...) *may be used as an element to demonstrate compliance*" with these requirements[619].

Data protection impact assessment (DPIA)

Finally, the controller must in certain situations, "*prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*", knowing that "*a single assessment may address a set of similar processing operations that present similar high risks*" [620]. These situations are those where the processing, "*in particular using new technologies,* (...) *is likely to result in a high risk to the rights and freedoms of natural persons*", taking into account "*the nature, scope, context and purposes*" of this processing[621]. As a consequence a DPIA "*will in particular be required in 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 of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale*" [622].

The Regulation does not contain any definition of data protection impact assessment, but requires that it contains at least the following[623]:

- "*a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller*";
- "*an assessment of the necessity and proportionality of the processing operations in relation to the purposes*";
- "*an assessment of the risks to the rights and freedoms of data subjects*"; and
- "*the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*".

In addition, "*where appropriate, the controller must seek the views of data subjects or their representatives on the intended processing*" [624], and reviews must be conducted where necessary "*to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*" [625].

---

[619] *Ibid.,* §3.

[620] Article 35 §1 of the General Data Protection Regulation.

[621] *Ibid.,* §1.

[622] *Ibid.,* §3.

[623] *Ibid.,* §7.

[624] *Ibid.,* §9.

[625] *Ibid.,* §11.

This mandatory content of any DPIA enables to conclude that "DPIA" is the new term for what was previously called "privacy impact assessment" (PIA), and which was used as an ethical practice in case a processing or more largely a project was likely to present risks for the right to privacy and personal data protection of natural persons, or more largely for fundamental rights[626].

Personal data processing for police purposes are subject to similar rules.

- The Council Framework Decision 2008/977/JHA provides for a right to compensation to be obtained "*from the controller or other authority competent under national law*"[627]. In addition, "*without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law*"[628]. Moreover, the Council Framework Decision makes logging and documentation mandatory, notably to ensure the data processing lawfulness[629]. Finally, Member States must "*adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision*", and must "*in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Framework Decision*"[630].
- Recommendation R. (87)15 of the Council of Europe Committee of Ministers does not provide for such provisions, except in the situation where the exercise of the right of access is refused[631]. However, several decisions of the ECtHR hold the liability of the State in case of data protection breaches by public authorities, on the basis of article 8 of the ECHR.[632]
- The new Police Directive contains similar principles as Directive 95/46/EC[633] but, in the same spirit than the new General Data Protection Regulation, clarifies and strengthens the controllers' liability and accountability (even if their obligations remain lighter than those of controllers who are subject to the Regulation).

[626] For a deeper development of this question, see the MANDOLA deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 11 July 2017.

[627] Article 19 of the Council Framework Decision.

[628] Article 20 of the Council Framework Decision.

[629] Article 10 of the Council Framework Decision. On this provision, see below our discussion relating to data security.

[630] Article 24 of the Council Framework Decision.

[631] Appendix to Recommendation R (87) 15, Principle 6.6: "*Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded*".

[632] See for instance See for instance ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §41, http://hudoc.echr.coe.int/eng?i=001-57533 (last accessed on 12 May 2017).

[633] In relation with the definition of the controller and processor see Art. 3 §8 and 9, and Art. 21 of the Police Directive.

Liability

The Directive develops that the data subject has the right to "*lodge a complaint with a supervisory authority*"[634], has the "*right to an effective judicial remedy against a supervisory authority*"[635], and has the "*right to an effective judicial remedy against a controller or a processor*[636]. The Police Directive also grants data subjects with a "*right to receive compensation* (...) *from the controller or processor*" [637] for any "*material or non-material damage* (suffered) *as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive*"[638]. Each supervisory or data protection authority is also empowered with several powers, including "*to monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures*", and to "*conduct investigations on the application of this Directive*"[639].

Accountability

In addition, the new Police Directive imposes to the controller, in the same terms as the Regulation, to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with*" the Directive, "*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*"[640]. These measures might include "*appropriate data protection policies*" [641].

Moreover, controllers have the duty to "*maintain a record of processing activities under their responsibility*" [642], which must contain a number of data listed such as the "*purposes of the processing*", the categories of recipients, of data subjects, of personal data, and "*where applicable, the use of profiling* (and) (...) *the categories of transfers of personal data to a third country or an international organisation*". Where possible, this record must also include "*envisaged times limits for erasure of the different categories of personal data*" and "*a general description of the technical and organisational security measures*"[643]. Each processor must itself "*maintain a record of all categories of*

[634] Article 52 of the new Police Directive.

[635] Article 53 of the new Police Directive.

[636] Article 54 of the new Police Directive.

[637] Article 56 of the new Police Directive.

[638] *Ibid.*

[639] Article 46 of the new Police Directive.

[640] Article 19, 1 of the new Police Directive. Article 4 relating to "principles relating to processing of personal data" also mentions in its §4 this principle of accountability: "*the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1, 2 and 3 ('accountability')*".

[641] Article 19, 2 of the new Police Directive.

[642] Article 24, §1 of the new Police Directive.

[643] *Ibid.,* §1.

processing activities carried out on behalf of a controller", also containing some listed information[644].

In addition, Member States must "*provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure*"[645]. The Directive clarifies that "*logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data*" [646]. These logs must "*be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings*" [647].

Data protection by design and by default

The controller must also ensure - in the same terms as the Regulation - "*data protection by design and by default*" [648], which means that he or her must, "*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 Directive and protect the rights of data subjects*"[649]. This must be done "*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*"[650]. Data protection by design and by default also means that the controller must "*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*"[651].

Data protection impact assessment (DPIA)

Finally, the controller must in certain situations, as well as controllers subject to the Regulation, "*carry out, prior to the processing, an assessment of the impact of the*

[644] *Ibid.,* §2.

[645] Article 25 §1 of the new Police Directive.

[646] *Ibid.,* §1.

[647] *Ibid.,* §2.

[648] Article 20 of the new Police Directive.

[649] *Ibid.,* §1.

[650] *Ibid.,* §1.

[651] *Ibid.,* §2.

envisaged processing operations on the protection of personal data"[652]. These situations are those where the processing, "*in particular, using new technologies,* (...) *is likely to result in a high risk to the rights and freedoms of natural persons*", taking into account "*the nature, scope, context and purposes*" of this processing[653].

The Directive does not contain any definition of data protection impact assessment, but requires that it contains at least the following[654]:

- "*a general description of the envisaged processing operations*";
- "*an assessment of the risks to the rights and freedoms of data subjects*", and;
- "*the measures envisaged to address the risks*", including "*safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of data subjects and other persons concerned*".

We can see that several steps that are necessary in a DPIA according to the Regulation disappear in the Directive, such as references to a legal compliance check and to an assessment of the necessity and proportionality of the processing operations, in other words to a ECHR compliance test. However, it must be noted that compliance with the Directive (which imposes to the controller to comply with the law implementing it) and with the ECHR imposes to Member States to ensure that these tests are performed.

Conclusion on the principle liability / accountability of the data controller

The MANDOLA consortium in relation with personal data processing performed during the MANDOLA research, as well as other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, must identify the data controllers who are responsible for the implementation of data protection rules, and these controllers have the duty to actually implement these rules.

The obligations of these controllers will be reinforced within the framework of the new General data protection Regulation, in terms of liability and accountability. They will have to ensure data protection by design and by default, and might be obliged to conduct a privacy impact assessment prior processing.

LEAs who would process personal data as a result of the use of the MANDOLA outcomes will have to identify the data controller who will be responsible for implementing their national data protection legislation. If a specific law has to be adopted to authorise the processing operations, it is recommended that this law takes into account the provisions of the new Police Directive, in order to ensure compliance with the future EU framework (notably by providing that the controller adopts policies and implements appropriate measures to ensure and be able to demonstrate that the personal data processing is performed in compliance with applicable law, both at the time of the determination of the means for processing and at the time of the processing itself;

[652] Article 27 §1 of the new Police Directive.

[653] *Ibid.,* §1.

[654] *Ibid.,* §2.

among these measures lie the maintaining of a record of processing activities under the controller's responsibility and record keeping of several processing operations. Privacy by design and by default will also have to be ensured, as well as the performance of a data protection impact assessment in situations where the processing operations are likely to present a high risk to the rights and freedoms of natural persons. Ideally, such DPIA should be performed before the law is voted in order to enable the law maker to include all appropriate safeguards in this law, ensuring this way compliance with ECHR requirements.

4.2.3.3.14 - Adequate level of protection in some case of data transfers

According to Directive 95/46/EC, the transfer of personal data to a third country may only take place if this third country "*ensures an adequate level of protection*", which shall be assessed "*in the light of all the circumstances surrounding (the) data transfer operation*", without prejudice to compliance with the other national provisions transposing the other provisions of the Directive[655]. Exceptions to this principle are allowed in a restrictive list of situations, which include *inter alia* the situation where "*the data subject has given his consent unambiguously*" and the situation where "*the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims*"[656].

The Data Protection Convention, in the same line, authorises a party to prohibit transborder flows where the receiving party does not provide equivalent personal data protection, and where the personal data are intended to be transferred to a non-contracting State through the territory of a party (circumventing that way the legislation of the sending party) [657].

The new General Data Protection Regulation contains similar principles, and brings some clarifications. The Regulation specifies that a transfer may take place, without any specific authorisation, "*where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection*"[658]. In the absence of a Commission's decision, "*a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*"[659]. These appropriate safeguards may be provided by several types of documents, some of them allowing a transfer "*without requiring any specific authorisation from a supervisory authority* (such as "*binding corporate rules*" or "*approved code of conduct*" accompanied with "*binding and enforceable commitments of the* controller (...) *in the third country to apply the appropriate safeguards*")[660], and some

[655] Article 25 of Directive 95/46/EC.

[656] Article 26 of Directive 95/46/EC.

[657] Article 12 of the Convention.

[658] Articles 45 §1 of the General Data Protection Regulation.

[659] Articles 46 §1 of the General Data Protection Regulation.

[660] *Ibid.* §2.

other allowing a transfer only if authorised by the competent supervisory authority (such as contractual clauses between the controller and the recipient of the personal data in the third country or international organisation)[661].

Derogations to these principles are allowed in a restrictive list of specific situations, which include *inter alia* the situation where the data subject has given an informed consent to the proposed transfer and the situation where "*the transfer is necessary for important reasons of public interest*"[662].

Personal data processing for police purposes are subject to similar rules, adapted to that particular sector.

- The Council Framework Decision 2008/977/JHA authorises transfers to competent authorities between Member States. Within this framework, where "*specific processing restrictions*" apply to data exchanges "*the transmitting authority shall inform the recipient of such restriction*", and "*the recipient shall ensure that these processing restrictions are met*"[663]. Additional conditions apply where the receiving Member State intends to transfer the personal data to private parties in its territory[664]. Transfers in third States or to international organisations may only take place if four conditions are fulfilled: (a) the transfer must be "*necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*"; (b) the receiving authority must competent to fulfil this same purpose; (c) "*the Member State from which the data were obtained* (must have) (...) *given its consent to transfer in compliance with its national law*" (unless serious threat to public security[665]), and (d) "*the third State or international body concerned* (must ensure) (...) *an adequate level of protection for the intended data processing*"[666]. If this fourth condition is not fulfilled, a short list of derogations include the existence of legitimate prevailing interests if the national law of the Member State transferring the data so provides and the providing by the receiving State of safeguards "*which are deemed adequate by the Member State concerned according to its national law*"[667]. The Council Framework Decision moreover provides guidelines in order to assess the "*adequacy of the level of protection*"[668].
- Recommendation R. (87)15 of the Council of Europe Committee of Ministers states that transfers between police bodies of data "*to be used for police purposes*" should only allowed "*if there exist a legitimate interest for such communication within the framework of the legal powers of these bodies*"[669]. Communication of data to other public bodies and to private parties "*should only be permissible*" if "*there exists a clear*

[661] *Ibid.* §3.

[662] Articles 49 of the General Data Protection Regulation.

[663] Article 12 of the Council Framework Decision.

[664] Article 14 of the Council Framework Decision.

[665] Article 13 §2 of the Council Framework Decision.

[666] Article 13 §1 of the Council Framework Decision.

[667] Article 13 §3 of the Council Framework Decision.

[668] Article 13 §4 of the Council Framework Decision.

[669] Appendix to Recommendation R (87) 15, Principle 5.1.

legal obligation or authorisation, or with the authorisation of the supervisory authority", or, for communications to public bodies, "*if these data are indispensable to the recipient to fulfil his own lawful task*", provided that the legal obligations of the communicating body and the principle of compatible use are respected[670]. Exceptions to these rules are exhaustively listed[671]. Finally, "*communication of data to foreign authorities should be restricted to police bodies. It should only be permissible (…). if there exists a clear legal provision under national or international* law", or, "*in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced*"[672]. The Recommendation also provides for conditions to be respected within the framework of requests for communication and of communication[673].

- The new Police Directive contains similar principles as the new Regulation. The Directive firstly specifies that a transfer may only take place in a particular framework which the Directive clarifies and which includes the requirement that the transfer is necessary for the purposes that are subject to this Directive[674] and that the recipient of personal data is an authority competent for these purposes. Within such a framework, Member States must "*provide that a transfer of personal data to a third country or an international organisation may take place* (without requiring specific authorisation) *where the Commission has decided that* (the latter) (...) *or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection*"[675]. In the absence of a decision from the Commission, Member States must "*provide that a transfer of personal data to a third country or an international organisation may take place where (a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data*"[676]. In this second case, the controller must "*inform the supervisory authority about categories of transfers*"[677] and the transfer must be documented and the documentation must be made available to the data protection authority on request[678].

[670] Appendix to Recommendation R (87) 15, Principles 5.2.i and 5.3.i.

[671] Appendix to Recommendation R (87) 15, Principles 5.2.ii and 5.3.ii.

[672] Appendix to Recommendation R (87) 15, Principle 5.4.

[673] Appendix to Recommendation R (87) 15, Principles 5.5.i and 5.5.ii.

[674] Art. 1§1 of the Directive: "*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*".

[675] Article 36 of the new Police Directive.

[676] Article 37 §1 of the new Police Directive.

[677] *Ibid.* §2.

[678] *Ibid.* §3.

Derogations to these principles are allowed in a restrictive list of specific situations, which include *inter alia* the situations where there is a need "*to protect the vital interests of the data subject or another person*" and where the purpose is "*the prevention of an immediate and serious threat to public security of a Member State or a third country*"[679].

Conclusion on the principle of adequate level of protection in case of data transfers

The MANDOLA partners who are data controller in relation with personal data processing performed during the MANDOLA research, as well as data controller of other natural or legal persons (other than competent authorities acting in crime prevention or repression) who would process personal data as a result of the use of the MANDOLA outcomes, must ensure that there is no data transfer to third countries that would not ensure an adequate level of data protection, unless they fall within one of the exceptions provided for by the EU and their national legislations**.** This principle will not be modified with the application of the new General Data Protection Regulation, even if the latter provides a more detailed framework for such transfers.

Within the framework of the potential use of the MANDOLA outcomes by LEAs, data controllers will also have to ensure to comply with their national legislation in terms of data transfer, which should *inter alia* ensure that transfer to third parties are allowed only if the receiving State ensures an adequate level of data protection, and that the transfer is necessary for the prevention of a serious and imminent danger or the suppression of a serious criminal offence. Transfers between Member States should also be reduced to a use for police purposes, be motivated by a legitimate interest for communication within the framework of the legal powers of concerned bodies, and receiving parties should respect any processing restrictions communicated by the transmitting authority. These principles will be reinforced with the application of the new Police Directive, since this text provides a more detailed framework for such transfers, with additional obligations (such as the documentation of certain kinds of transfer), and since all the other principles of the new Police Directive will apply to data transfers, which are a kind of data processing.

4.2.3.3.15 - General conclusion on the substance of personal data protection

Fourteen general principles have been studied in the current section. These principles, common to four legal instruments applicable to the MANDOLA consortium and/or to law enforcement authorities (the Council of Europe Data Protection Convention, taking into account the proposals for a modification of this Convention, the EU Directives 95/46/EC and 2002/58/EC, Recommendation (87) 15 of the Committee of Ministers of the Council of Europe, and the Council Framework Decision 2008/977/JHA), are the following:

1. Legal basis
2. Legitimate, explicit and specified purpose
3. Data quality
4. Data minimisation

[679] Article 38 of the new Police Directive.

5. Time limitation
6. Data subject's consent or other appropriate legal ground
7. Data subject information
8. Data subjects' rights of access, communication, rectification and erasure
9. Prohibition of automated decisions
10. Enhanced protection of some sensitive data
11. Security and confidentiality of the processing
12. Data protection authority supervision
13. Liability and accountability of the controller
14. Adequate level of protection in some case of data transfers

These fourteen general principles must be respected both by the MANDOLA consortium and by other entities, including law enforcement agencies, that would use the MANDOLA outcomes at the end of the MANDOLA project, where the further development or where the use of these outcomes implies personal data processing operations. As targeted in the short conclusions proposed at the end of the analysis of each of these principles, these principles may apply in a different way and may have different practical implications, depending on whether the processing is carried out by the private sector for the purpose of scientific research or by police services for the purpose of crime prevention, and depending on the date of the processing, since the new EU framework on personal data protection will be applicable in May 2018.

However, as it can be seen from our short conclusions that follow the study of the afore-mentioned principles, the provisions of this future EU legal framework:

- May be in some situations already applied by the MANDOLA consortium, under an ethical approach, where they clarify a current legal framework that is currently less explicit, or where they enhance the protection of citizens' rights, in addition to, in both cases, obviously complying with the ECHR principles as interpreted by the ECtHR in relation to the protection of privacy and personal data, since the latter principles also apply to personal data processing and must themselves be taken into account and respected[680].
- Should be taken into account within the context of the drawing up of the legal bases that might have to be adopted, at national levels, to authorise personal data processing implied by the use of the MANDOLA outcomes, where these new principles clarify a current legal framework that is currently less explicit or enhance citizens' rights. This, firstly to ensure compliance with the future legal framework.

Finally, it has to be noted that the current section related to the substance of personal data protection did not cover obligations that are not applicable to the MANDOLA consortium or to law enforcement agencies within the framework of the use of MANDOLA outcomes, such as particular obligations, provided for in the General Data Protection Regulation and the Police Directive on the processing of personal data for the purpose of crime prevention, concerning controllers not established in the EU or controllers who offer goods and services directly to a child.

[680] These principles are studied in our Section 4.1.3..

4.3 Freedom of expression

Understanding the right to freedom of expression requires addressing the protecting legal instruments of this right, the notion of freedom of expression, and the nature and extent of freedom of expression. These issues will be the subject of a comparative study since freedom of expression being the first of the rights that are impacted by the prohibition of hate speech, its detailed study appears to be of utmost importance.

4.3.1 Legal instruments protecting the freedom of expression

As well as the other rights studied in this report, the right to freedom of expression is protected on one hand by International and European texts, and on the other hand by national constitutions and laws.

4.3.1.1 International and European instruments

At the international level, the right to freedom of expression is notably declared by Article 19 of the United Nations Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, and Article 10 of the European Convention on Human Right (ECHR). At the European level, it is protected by Article 11 of the EU Charter of Fundamental rights (EUCFR). As a result freedom of expression is a Human Right and a Fundamental Freedom, and therefore, in numerous States, a Civil Liberty. It applies to adults and children, even if the United Nations Convention on the Rights of the Child supplements this with a specific declaration on children's right to freedom of expression in Article 13.

4.3.1.2 National Constitutions

Freedom of expression is moreover protected by several national Constitutions, and by all the ones of the ten countries that have been studied in the course of the MANDOLA project.

In Belgium, freedom of expression is protected by Articles 19[681] and 25[682] of the Constitution, Article 25 being particularly devoted to the freedom of the press.

In Bulgaria, freedom of expression is protected by Articles 39 to 41 of the Constitution[683].

---

[681] **Article 19:** "*Freedom of worship, its public practice and freedom to demonstrate one's opinions on all matters are guaranteed, but offences committed when this freedom is used may be punished*."

[682] **Article 25:** "*The press is free; censorship can never be introduced; no security can be demanded from authors, publishers or printers. When the author is known and resident in Belgium, neither the publisher, the printer nor the distributor can be prosecuted*."

[683] **Article 39:** *"(1) Everyone shall have the right to express an opinion or to disseminate an opinion by means of words - whether in writing or orally, through sound, image, or by any other medium. (2) This right may not be used to the detriment of the rights and reputation of others, or to call for a forcible change of the constitutionally established order, for the commission of criminal offences, or for incitement to animosity or for personal violence*". **Article 40:** *"(1) The press and the other mass communication media shall be free and shall not be subject to censorship. (2) A suppression and seizure of a print publication or of another information medium shall be admissible solely in pursuance of an instrument of the judiciary, where good morals are impaired or the publication contains calls for a forcible change of the constitutionally established order, for the commission of a criminal offence, or for personal violence. Unless seizure follows within 24 hours, the effect of any such suppression shall lapse*". **Article 41:** "*1. Everyone shall be entitled to seek, obtain and disseminate information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality. 2. Everyone shall be entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or*

In Cyprus, freedom of expression is protected by Article 19 of the Constitution[684].

In France, freedom of expression is protected by Article 11 of the Declaration of Human and Citizen's Rights of 1789[685], which belongs to the French "Constitutional bloc".

In Germany, freedom of expression is protected by Article 5 (1) of the Constitution ('*Grundgesetz*')[686].

In Greece, freedom of expression is protected by Articles 14 (1) and 5A[687].

In Ireland, Freedom of expression is protected by Article 40.6.1 of the Constitution[688].

In the Netherlands, freedom of expression is protected by Article 7 of the Constitution[689].

---

official secret and does not affect the rights of others". An English translation of the Bulgarian Constitution is available at https://www.constituteproject.org/constitution/Bulgaria_2007.pdf?lang=en (last accessed on 30 May 2017).

[684] **Article 19:** "*1.Every person has the right to freedom of speech and expression in any form. 2. This right includes freedom to hold opinions and receive and impart information and ideas without interference by any public authority and regardless of frontiers. 3. The exercise of the rights provided in paragraphs 1 and 2 of this Article may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the reputation or rights of others or for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary*". Moreover **Art. 12 (3)** of the constitution states: "*No law shall provide for a punishment which is disproportionate to the gravity of the offence*".

[685] **Article 11**: "*The free communication of ideas and opinions is one of the most precious rights of man. Every citizen may thus speak, write and publish freely, except when such freedom is misused in cases determined by Law*". An English translation of this Declaration is available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/cst2.pdf (last accessed on 30 May 2017).

[686] **Article 5 [Freedom of expression, arts and sciences]:** *"(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship. (2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour. (3) Arts and sciences, research and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution*".

[687] **Article 14 (1)** provides that every person may express and propagate his or her thoughts orally, in writing and through the press, in compliance with the laws of the State. **Article 5A** states: "*1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19*".

[688] **Article 40.6. 1°:** "*The State guarantees liberty for the exercise of the following rights, subject to public order and morality: i The right of the citizens to express freely their convictions and opinions* (...)".

[689] **Article 7:** "*1. No one shall require prior permission to publish thoughts or opinions through the press, without prejudice to the responsibility of every person under the law. 2. Rules concerning radio and television shall be laid down by Act of Parliament. There shall be no prior supervision of the content of a radio or television broadcast. 3. No one shall be required to submit thoughts or opinions for prior approval in order to disseminate them by means other than those mentioned in the preceding paragraphs, without prejudice to the responsibility of every person under the law. The holding of performances open to persons younger than sixteen years of age may be regulated by Act of Parliament in order to protect good morals. 4. The preceding paragraphs do not apply to commercial advertising.*"

In Romania, freedom of expression is protected by Article 30 of the Constitution[690].

In Spain, freedom of expression is protected by article 20 of the Constitution[691].

4.3.2 The notion of freedom of expression

At the Council of Europe and EU levels, freedom of expression is considered to be an essential foundation of a democratic society. In terms of content, the right to freedom of expression includes "*freedom to hold opinions and to receive and impart information and ideas without interference (...) and regardless of frontiers*"[692]. In other words the right to freedom of expression includes primarily the right to communication and the right to information. It also includes a right to freedom of media, and a right to access the Internet.

4.3.2.1 An essential foundation of a democratic society

According to the ECtHR, the right to freedom of expression "*constitutes one of the essential foundations of* (...) (a democratic) *society, one of the basic conditions for its progress and for the development of every man*"[693]. This right is "*applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population*"[694]. The Court explains that "*such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'*"[695]. This approach is also the one of the EU, which can be summarised by quoting the EU Parliament: "*freedom of expression in the public*

---

[690] **Article 30:** "*(1) Freedom of expression of thoughts, opinions, or beliefs, and freedom of any creation, by words, in writing, in pictures, by sounds or other means of communication in public are inviolable. (2) Any censorship shall be prohibited. (3) Freedom of the press also involves the free setting up of publications. (4) No publication shall be suppressed. (5) The law may impose upon the mass media the obligation to make public their financing source. (6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of a person, and to the right to one's own image. (7) Any defamation of the country and the nation, any instigation to a war of aggression, to national, racial, class or religious hatred, any incitement to discrimination, territorial separatism, or public violence, as well as any obscene conduct contrary to morality shall be prohibited by law. (8) Civil liability for any information or creation made public falls upon the publisher or producer, the author, the producer of the artistic performance, the owner of the copying facilities, radio or television station, under the terms laid down by law. Indictable offences of the press shall be established by law*". The Romanian Constitution is available in English at: http://www.cdep.ro/pls/dic/site.page?id=371.

[691] **Article 20:** "*1. The following rights are recognised and protected: a) the right to freely express and disseminate thoughts, ideas and opinions trough words, in writing or by any other means of communication; b) the right to literary, artistic, scientific and technical production and creation; c) the right to academic freedom; d) the right to freely communicate or receive accurate information by any means of dissemination whatsoever. 2. The exercise of these rights may not be restricted by any form of prior censorship. 3. The law shall regulate the organisation and parliamentary control of the social communications media under the control of the State or any public agency and shall guarantee access to such media to the main social and political groups, respecting the pluralism of society and of the various languages of Spain. 4. These freedoms are limited by respect for the rights recognised in this Title, by the legal provisions implementing it, and especially by the right to honour, to privacy, to personal reputation and to the protection of youth and childhood. 5. The confiscation of publications and recordings and other information media may only be carried out by means of a court order*".

[692] Article 10§1 of the ECHR.

[693] ECtHR, plen., 7 December 1976, *Handyside v. The United Kingdom*, §49, http://hudoc.echr.coe.int/eng?i=001-57499 (Last accessed on 24 May 2017).

[694] *Ibid.*

[695] *Ibid.*

sphere has been shown to be formative of democracy and the rule of law itself, and coaxial to its existence and survival"[696].

Even if these provisions and interpretation are applicable in the ten EU countries that have been studied during the MANDOLA research, constitutional Courts do not recognise the importance of this right the same way. However, these differences of formal recognition do not prejudice how and the extent to which the right is protected in practice[697].

- In five countries, Constitutional Courts protect the right to freedom of expression by verifying if the conditions for its limitations are respected, without particularly considering this right as being of higher importance than the other fundamental rights. This is the case in Belgium[698], in Bulgaria, in Ireland, and in the Netherlands[699].
- In some other countries, Constitutional courts expressly give to freedom of expression a particular importance:
  - **In Cyprus,** the Supreme Court has constantly affirmed a status of reinforced protection for the right of freedom of expression, which is characterised as a blessing and a feature of every civilized society[700].
  - **In France**, the Constitutional Council considers that "*freedom of expression and communication are all the more precious since they are one of the cornerstones of a democratic society and one of the guarantees of respect for other rights and freedoms*"[701].
  - **In Germany**, the Constitutional Court considers that "*the fundamental right to freedom of expression is as a direct expression of human personality, one of the noblest human rights in society (...). To a free and democratic state, it is essential because it facilitates continuous intellectual controversy, the "clash of opinions" which is a free democratic state's primary element. It is, in a way, the very basis*

[696] European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), B, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203 (last accessed on 30 May 2017).

[697] See our Section 4.3.3.

[698] In Belgium the Court of cassation considers that freedom of expression is a constitutional right that can be subject to certain limitation or sanction under particular conditions only: Decision of 25 April 2007, N° C.06.0123.N, 1.H. R., 2.G. E. v. D. J., http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20070427-2 (last accessed on 26 May 2017 - might have to be modified into a pdf file).

[699] However, a representative of the judiciary has considered this right to fulfil "an essential role in public debate in a democratic society"Martijn de Koning, "Netherlands", in Jørgen Nielse et al., *Yearbook of Muslins in Europe*, vol. 3, Brill, 2011, p.416, referring to a Dutch public prosecutor comment.

[700] Supreme Court, Georgios Chatzinicolaou v Police (1976) 2 C.L.R. 63.

[701] See for example French Constitutional Council, Decision n° 2015-512 QPC of 8 January 2016, §5, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2015-512-qpc/decision-n-2015-512-qpc-du-8-janvier-2016.146840.html; Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 15, available in English at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf (URLs last accessed on 26 May 2017).

of freedom, 'the matrix, the indispensable condition of nearly every other form of freedom"[702].

- **In Greece**, the Council of State (the Greek Supreme Administrative Court) considers freedom of expression as a fundamental right in a democratic society[703].
- **In Romania**, the Supreme Court recognises that the ECtHR "*emphasises the importance of freedom of expression, considered to be 'one of the essential foundations of a democratic society'*"[704].
- **In Spain**, the freedom of speech has been considered as "essential for democracy" and is placed "in a unique position when compared to other rights"[705]. In particular, the Constitutional Court considers that freedom of expression has a prevalent interest over the right of honour[706].

4.3.2.2 The right to receive and impart information

The right to freedom of expression implies a right of communication of individuals between themselves[707], and a corresponding right to receive information[708], especially where the information is of public interest[709]. States have the positive obligation to protect these

[702] Germany: Lüth case, https://www.article19.org/resources.php/resource/3202/en/germany:-l%C3%BCth-case, referring to the Lüth case, BVerfGE 7, 198; 1 BvR 400/51 of January 15, 1958 ("Cardozo - p. 208, references omitted") (URL last accessed on 26 May 2017).

[703] Council of State 3880/2002, *HellDik* 2004, 1275. See also Council of State 832/1985; 2109/1988; 3938/1988; 1824/1989; 199/1991.

[704] Decision n°206, 29 April 2013, published in the Official Gazette of Romania, Part I, n°350 of 13 June 2013, with the correction published in the Official Gazette of Romania, Part I, n°380 of 27 June 2013p. 3, available in English at https://www.ccr.ro/files/products/Decizie_206_2013en.pdf (last accessed on 30 May 2017).

[705] Enrique Guillen Lopez, *Judicial Review in Spain: The Constitutional Court*, Loyola of Los Angeles Law Review, 1 January 2008, p.22, http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=2616&context=llr (last accessed on 26 May 2017).

[706] Decision 51/1989. Moreover, there are some relevant interests that must be taken into consideration: the public interest of information (Decisions 21/2000, 46/2002 and 54/2004); the persons spoken about in the news (Decisions 278/2005 and 9/2007), and the difference between information and opinion (decisions 54/2004, 53/2006 and 139/2007). There is an important issue concerning these interests: when the individual is of great public relevance, and when the activity he/she carries out takes place in the public sphere (Decisions 224/1999 and 231/1988). In addition, the restriction to the freedom of expression also affects the personal intimacy: the public projection of the person involved (Decision 81/2001, Emilio Aragón case), the space where the images have been shown (public or private place) and if the consent has been given by the subject involved (Decision 139/2001, Marta Chávarri case).

[707] ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity*, Council of Europe/European Court of Human Rights, December 2011, p. 4, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf (last accessed on 30 May 2017).

[708] Article 10 of the ECHR.

[709] The ECtHR evokes the right for the public to receive "*information and ideas on matter of public interest*": ECtHR, plen., 26 November 1991, *Observer and Guardian v. The United Kingdom*, appl. n°13585/88, §59, http://hudoc.echr.coe.int/eng?i=001-57705 (last accessed on 26 May 2017).

rights, "*even in the sphere of relations between individuals*" [710]. This "*horizontal effect*" [711] of the Convention implies inter alia for the States to "*foster as much as possible a variety of media and a plurality of information sources, thereby allowing a plurality of ideas and opinions*"[712].

This requirement of pluralism of media, which gives consistency to the freedom to be informed, is also expressly mentioned in the EU Charter of Fundamental Rights in Article 11, §2[713]. This requirement is based, in particular, *"on Court of Justice case law regarding television"*[714], *"on the Protocol on the system of public broadcasting in the Member States annexed to the EC Treaty and now to the Constitution, and on Council Directive 89/552/EC (particularly its seventeenth recital)"*[715].

These principles apply in all the ten EU countries that have been studied during the MANDOLA project, but the Constitutional (and related) courts still remain globally silent on the State's positive obligation of fostering pluralism in relation with freedom of expression, except in France[716]. Six of these countries emphasise both aspects of the right to freedom of

[710] ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, op. cit.* p. 4.

[711] ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, op. cit.* p. 4; Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 9, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (last accessed on 12 May 2017).

[712] Council of Europe, Committee of Ministers, Declaration on the freedom of expression and information, 29 April 1982, n°6, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016,* §6 p. 272, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (last accessed on 24 May 2017). See also ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, op. cit.* p. 4.

[713] Article 11§2: "*the freedom and pluralism of the media shall be respected*".

[714] Particularly CJEU; 25 July 1991, *Stichting Collectieve Antennevoorziening Gouda and others v. Commissariaat voor de Media*, Case C-288/89, esp. §23, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61989CJ0288. Quotation from European parliament, *Explanations relating to the Charter of Fundamental Rights of the European union*, Art. 11, §2, available from http://www.europarl.europa.eu/charter/convent49_en.htm and at http://www.europarl.europa.eu/charter/pdf/04473_en.pdf (URLs last accessed on 30 May 2017).

[715] European parliament, *Explanations relating to the Charter of Fundamental Rights of the European union*, *op. cit*.

[716] The Constitutional Council declared that the "*pluralism of daily newspapers (...) is itself an objective of Constitutional value*"(1) which ensures "*the efficiency of the declared freedom: indeed, it is useless to ensure the freedom to express oneself, in a democratic society, if the public accesses only one rhetoric*"(2). The general public, "*primary user*" of the right to freedom of expression(1), must "*have available a sufficient number of publications of different trends and types*"(1) and be "*able to exercise their free choice being protected against the possibility for public authorities or private interests to substitute their own decisions to this choice, and against the possibility to make this choice the subject of a contract*"(1). Freedom of press efficiency will be especially ensured by financial transparency, which implies the possibility, for the reader, to have knowledge about the actual directors of press companies, the newspapers financing conditions, the financial transactions the latter may be the subject of, and about all kind of interests involved" (3). **(1)** Decision n° 84-181 DC of 11 October 1984, §38, http://www.conseil-constitutionnel.fr/conseil-con..decision-n-84-181-dc-du-11-octobre-1984.8135.html; **(2)** Bertrand Lamy, *La liberté d'expression et de communication*, Dossier, Nouveaux cahiers du Conseil constitutionnel n°36, June 2012, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-36/la-constitution-et-la-liberte-de-la-

expression that are the right to communicate ideas and opinions and the right to receive information (Bulgaria[717], Belgium[718], France[719], Cyprus[720], Spain[721], Greece[722]), while four countries are more obscure or did not have the occasion to pronounce a decision on the existence of a right to receive and access information (Germany[723], the Netherlands, Ireland, and Romania).

4.3.2.3 Rights to confidence, education and reply in relation to expression and information

The right to express one's opinion is primarily a right to expression without fear and to be able to reply to information already published. The right to receive information is primarily a right to receive truthful information, since in order to participate in the public debate citizens must be adequately informed. In this sense, the positive obligation of States to ensure the effectiveness of the right to freedom of expression implies to gives citizens the confidence that they can express themselves without fear[724], to enable them to reply to published information[725] and to give them the skills and critical attitude that enable them to

presse.114758.html; **(3)** Bertrand Lamy, op. cit., referring to Decision n° 84-181 DC of 11 October 1984, §16, *op.cit*. Sources translated from French, URLs last accessed on 30 May 2017.

[717] Both rights are mentioned in the Constitution.

[718] In Belgium the Constitution is silent on this but the Court of cassation mentions explicitly the right to receive information under art. 10 of the ECHR in the discussion that bases his judgement: see Decision of 25 April 2007, N° C.06.0123.N, 1.H. R., 2.G. E., contre D. J., p.4, http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20070427-2 (last accessed on 26 May 2017 - might have to be modified into a pdf file).

[719] In France, freedom of expression includes the "*freedom of expression and communication*"(1), including "*the free communication of ideas and opinions*"(2), and as a consequence the possibility for every citizen to "*speak, write and publish freely*", subject to legal limitations (2). (1): See for example French Constitutional Council, Decision n° 2015-512 QPC of 8 January 2016, §5, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2015-512-qpc/decision-n-2015-512-qpc-du-8-janvier-2016.146840.html; Decision n° 2009-580 DC of 10 June 2009, § 15, available in English at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf; (2): Article 11 of the Declaration of Human and Citizen's Rights of 1789, which belongs to the French "Constitutional bloc" (an English translation of this Declaration is available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/cst2.pdf) (URLs last accessed on 30 May 2017).

[720] Both rights are mentioned in the Constitution.

[721] Both rights are mentioned in the Constitution and confirmed by the Constitutional Court (see for ex. decisions n° 51/1989; 197/1982; 217/1992, and 52/2002.

[722] Art. 5A 1 of the Constitution (see our Section 4.3.1.2)

[723] The German Constitution evokes the right for everyone to inform himself or herself "*without hindrance from generally accessible sources*" (art. 5).

[724] ECtHR, 2nd Sect., 14 September 2010, *Dink v. Turkey*, appl. n°s 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09, §137, http://hudoc.echr.coe.int/eng?i=001-100384; ECtHR, *Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity*, Council of Europe/European Court of Human Rights, December 2011, p. 5, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf (URLs last accessed on 30 May 2017)..

[725] ECtHR, 2nd Sect., 5 July 2005, *Melnychuk v. Ukraine (dec.)*, appl. n°. 28743/03, http://hudoc.echr.coe.int/eng?i=002-3781; ECtHR, *Research report: positive obligations on member states*

face and understand the information they receive, including where this information is harmful to them, to distinguish between true and false information, to understand the benefits and the risks of measures aiming at regulating Internet content and to have a democratic and responsible attitude respecting the rights of others. The latter right of education is of particular importance and has been especially highlighted in several recommendations of the Council of Europe Committee of Ministers[726] as well as by the European Parliament[727].

These rights are naturally enforceable in the ten EU countries that have been studied during the MANDOLA project, as well as in the other EU and Council of Europe States parties. However, it must be noted that in one of the studied countries, namely Germany[728], the right to access truthful information takes the form of a non-protection of the access to false information. Such kind of statement, depending on the way it is interpreted and applied, might present the risk to lead to censorship depending on the persons or entities authorised to qualify the information as being false, and might even be detrimental to the right of information through media providing transparently false information in order to denounce ironically topical subjects[729].

---

under Article 10 to protect journalists and prevent impunity, *op. cit.* p. 5; Recommendation of the Committee of Ministers of the Council of Europe on the right to reply in the new media environment, 15 December 2004, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016,* p. 119, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (last accessed on 24 May 2017).

[726] Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, op. cit.*, p 288 and http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp; In the same document see Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, p. 150 quot. p. 152, see also p. 153; Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, 27 September 2006, p. 124; Appendix to Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, p 162, part III, especially pp. 164 *et seq*.

[727] European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), n°30, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203 (last accessed on 30 May 2017)

[728] Constitutional Court, 'CSU: NPD of Europe' decision (BVerfGE 25, 256); see also the "Holocaust Denial" decision (BVerfGE 90, 241) in which the denial of the holocaust is a representation of false facts that does not enjoy the protection freedom of speech.

[729] Such as the Gorafi in France (http://www.legorafi.fr), Nordpresse in Belgium (http://nordpresse.be/) or Waterford whispers news in Ireland (http://waterfordwhispersnews.com). A Wikipedia webpage gives a list of numerous of them: https://en.wikipedia.org/wiki/List_of_satirical_news_websites.

4.3.2.4 Freedom of press and media

The right to receive and impart information implies a right to freedom of press and media, which have a "*vital public-watchdog role*"[730]. Therefore, "*safeguards to be afforded to the press are of particular importance*"[731] and "*Protection of journalistic sources is one of the basic conditions for press freedom*"[732]. Without such protection, "*sources may be deterred from assisting the press in informing the public on matters of public interest*" [733]; As a result, the "*role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected*" [734]. The importance of the protection of sources, including in times of crisis has been further highlighted by the Council of Europe Committee of ministers[735].

This approach is also the one of the EU, which can be summarised by quoting the EU Parliament: "*freedom of the media is a cornerstone of the values enshrined in the Treaties, among them democracy, pluralism, and respect for the rights of minorities; whereas the history thereof, under the name of 'freedom of the press' has been constitutive of the progress of democratic ideas and the development of the European ideal in history*" [736].

In addition, the Council of Europe Committee of Ministers recommends to "*adopt a new, broad notion of media which encompasses all actors involved in the production and dissemination, to potentially large numbers of people, of content (for example information, analysis, comment, opinion, education, culture, art and entertainment in text, audio, visual, audiovisual or other form) and applications which are designed to facilitate interactive mass communication (for example social networks) or other content-based large-scale interactive experiences (for example online games)*"[737]. The European Parliament is on the same line, underlining the importance of ensuring "*the fundamental right to freedom of expression* (in) (...) *social media and other forms of new media* (...) *notably through guaranteeing net neutrality* (...) (and) *the unrestricted access to and provision and circulation of information* (...) (without for authorities to attempt) *to require registration or authorisation or curb*

---

[730] ECtHR, gr.ch., 27 March 1996, Goodwin v. United Kingdom, appl. no17488/90, §39, http://hudoc.echr.coe.int/eng?i=001-57974 (last accessed on 18 May 2017).

[731] *Ibid.* § 39.

[732] *Ibid.* § 39.

[733] *Ibid.* § 39.

[734] *Ibid.* § 39.

[735] See for ex. Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression in times of crisis, 26 September 2007, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016,* p. 138, esp. p 140, n°13, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (last accessed on 24 May 2017).

[736] European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), B, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203 (last accessed on 30 May 2017).

[737] Appendix to the recommendation CM/Rec(2007)16 of the Committee of Ministers to Member States on measures to promote the public service value of the Internet, 7 November 2007, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, op.cit.,* p. 166 quot. p. 167.

content alleged by them to be harmful"[738]. The Parliament also acknowledges that "*the provision of internet services by public service media contributes to their mission of ensuring that citizens are able to access information and form their opinions from a variety of sources*" [739], and calls for the inclusion of "*news aggregators, search engines and other intermediaries in the dissemination of and access to information and news content on the internet* (...) *in the* (future) *EU regulatory framework* (...) *in order to tackle the problems of discrimination of content and distortion of source selection*"[740].

The freedom of press is formally protected in all the ten EU countries that have been studied. This protection is based on the Constitution (Belgium, Bulgaria, France[741], Germany, Greece[742], the Netherlands, Romania and Spain[743]) or on a decision of the Supreme Court (such as in Cyprus[744]) or of the Constitutional Court (Ireland[745]). It is however restricted to print media in Greece[746], and, in a lesser extent, in Spain[747].

---

[738] European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU, *op. cit.,* §28.

[739] *Ibid.* §28.

[740] *Ibid.* §29.

[741] Article 11 of the Declaration of Human and Citizen's Rights of 1789 does not mention the "press" but evokes the right to "speak, write and publish freely", which is traditionally considered to refer to press (see for ex. Bertrand Lamy, *La liberté d'expression et de communication*, Dossier, Nouveaux cahiers du Conseil constitutionnel n°36, June 2012, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-36/la-constitution-et-la-liberte-de-la-presse.114758.html - last accessed on 30 May 2017).

[742] The Council of State (the Greek Supreme Administrative Court) has held that the constitutional provisions establish the fundamental for every democratic society right of freedom of expression and dissemination of ideas, particularly through the Press: Council of State 3880/2002, HellDik 2004, 1275. See also Council of State 832/1985; 2109/1988; 3938/1988; 1824/1989; 199/1991.

[743] Article 20 of the Constitution does not refer to "press" but it is traditionally considered to include the freedom of press.

[744] The Supreme Court protects freedom of press based on Article 19 of the Constitution, by reference to the ECtHR jurisprudence: see Cosmos Press Ltd and Another v The Police (1985) 2 CLR 73.

[745] See for ex. Supreme Court, *Mahon Tribunal v. Keena & anor*, 31 July 2009, [2009] IESC 64, §19, http://www.supremecourt.ie/Judgments.nsf/60f9f366f10958d1802572ba003d3f45/90870229324e38bb80257604003c74c2?OpenDocument (last accessed on 30 May 2017), which also mentions that "*the preservation from disclosure of journalistic sources, as an essential prerequisite of a free press in a democratic society*".

[746] The protection of the Constitution is restricted to the printed media and does not extend to electronic mass media. In particular, Article 15 (1) states that: "the protective provisions for the press in the preceding article shall not be applicable to films, sound recordings, radio, television or any other similar medium for the transmission of speech or images", while Article 15 (2) provides that radio and television shall be under the direct control of the State.

[747] The Spanish Constitutional Court makes a difference between written media of which the creation is totally free, and media that needed technical support, to which the legislator can apply technical limitations and make decisions in relation to their impact on the public opinion. The legislator is also responsible for making a decision between (a) a public monopoly ruled by the constitutional guarantees (mentioned in art.20.3 Constitution) and (b) a free access by private companies following the terms established by the legislator in other regulations (Decision 12/1982 of 31 March 1982): Ascensión Elvira Perales, Profesora Titular. Universidad Carlos III. Diciembre 2003. Actualizada por Ángeles González Escudero, Letrada de las Cortes Generales. Enero 2011, http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=20&tipo=2.

4.3.2.5 The protection of the access to the Internet

Article 10 of the ECHR applies to the Internet as a means of communication[748], which means that "*freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form*"[749].

In addition, access to the Internet is itself protected as a means of exercising freedom of expression, at the Council of Europe level[750] as well as at the European level[751]. As a consequence, "*State interference in the form of blocking or restricting access to the Internet is subject to strict scrutiny*" by the ECtHR[752].

These principles are, as well as the previous ones that have been analysed, applicable in the EU countries and particularly in the ten EU Member States that have been studied during the MANDOLA projects. However, their recognition at national levels is still incomplete.

- The equal treatment of digital and non-digital environment is recognised by the Constitution[753] or by Courts as included in the principle of freedom of expression protected by the Constitution[754] in all the studied countries. However, freedom of media is partly restricted in Greece, and, in a lesser extent, in Spain[755].

---

[748] ECtHR, gr. ch., 16 June 2015, *Delfi AS v. Estonia*, appl. n°64569/09, § 131, http://hudoc.echr.coe.int/eng?i=001-155105; ECtHR, Research division, *Internet: case-law of the European court of Human Rights*, updated June 2015, p.17, http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (URLs last accessed on 24 May 2017).

[749] Council of Europe, Committee of Ministers, Declaration on human rights and the rule of law in the Information society, available in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, op. cit.,* p. 288, quot. p. 289.

[750] "the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general" and blocking Internet access may be "*in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured 'regardless of frontiers'*": see ECtHR, 2nd Sect., 18 December 2012, *Ahmet Yıldırım v. Turkey*, appl. n°3111/10, respectively §48 and §67, http://hudoc.echr.coe.int/eng?i=001-115705; ECtHR, Research division, *Internet: case-law of the European court of Human Rights*, *op. cit.* p. 22 and pp.44-45; see also Appendix to the recommendation CM/Rec(2007)16 of the Committee of Ministers to Member States on measures to promote the public service value of the Internet, in *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, op. cit.*, p. 150.

[751] See for example European Parliament resolution of 10 April 2008 on cultural industries in Europe, 2007/2153(INI), § 23, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN; Estelle De Marco in Cormac Callanan, Marco Gercke, Estelle De Marco and Hein Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, p. 258, http://www.aconite.com/blocking/study (French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/) (URLs last accessed on 24 May 2017).

[752] ECtHR, Research division, Internet: case-law of the European court of Human Rights, updated June 2015, *op. cit.* p. 46.

[753] Such as in Bulgaria (Article 39 of the Constitution mentioning "*any other medium*") and in Greece (where provisions relating to freedom of expression apply as well on any media).

[754] Such as in Belgium, in Cyprus, in France, in Germany, in Ireland, in the Netherlands, in Romania and in Spain.

[755] See our Section 4.3.2.5.

- The freedom to access the Internet is recognised in Belgium[756], in France[757], in Greece[758] and - in a lesser extent - in Germany[759], but is not the subject of an explicit legal provision or court's decision in Bulgaria, Cyprus, Ireland, the Netherlands, Romania, and Spain[760].

4.3.3 Nature and extent of the freedom of expression

The nature and extent of the protection of the right to freedom of expression might still differ between the one offered by the ECtHR and the ones applied at States parties' national levels.

4.3.3.1 The ECtHR protection

At the ECHR level, general requirements for limiting conditional rights[761] apply but are subject to adaptations in order to answer the particularities of the freedom of expression.

4.3.3.1.1 Application of the general requirements for limiting conditional rights

In the same way as for the protection of the right to private life[762], the protection of the right to freedom of expression is ensured by the European Union Court of Justice (EUCJ) on

---

[756] In Belgium, the "freedom to access the Internet" is not particularly protected but the Belgian Government has put in place a strategy (named 'Digital Belgium 2015-2010) based upon the statement that each person residing in Belgium has the right to have access to the Internet (http://economie.fgov.be/fr/binaries/Plan_internet_tres_haut_debit_Belgique_tcm326-275861.pdf). Therefore a right to access the Internet does exist, even though it is not formally considered to be based on the right to freedom of expression.

[757] Constitutional Council, Decision 2009-580 DC of 10 June 2009, JO of 13 June 2009, p. 9675, http://www.conseil-constitutionnel.fr/decision//2009/decisions-pardate/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html, recital 12 : "*In the current state of communication means and taking into account both the general development of online public communication means and the importance of these services for the participation in democratic life and for the flow of ideas and opinions, (the right to freedom of expression) implies the freedom to access these services*".

[758] On the basis of art. 14 (1) of the Constitution: see P. Dagtoglou, Constitutional Law. Civil Rights, A, (Sakkoulas, 2012, in Greek), 415; Mantzoufas, Freedom of expression and the Internet, http://www.constitutionalism.gr/1834-eleyteria-ekfrasis-kai-diadiktyo/ (in Greek). In addition, Article 5A§2 of the Constitution states: "*all persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19*". This provision can be interpreted as protecting against restrictions to the access to the Internet but there is no case law applying this constitutional provision in this context.

[759] In Germany the freedom to access the internet is not specifically protected, neither by substantive nor by constitutional law, but the general freedom to information without hindrance provided by the Constitution can serve as a basis for such a freedom.

[760] However, there are in Spain some proposals for both protecting the access to Internet as part of article 20 of the Constitution relating to freedom of expression and protecting the right to be forgotten as part of article 18 of the Constitution relating to the right to intimacy: see Sánchez, 2015. http://www.eldiario.es/hojaderouter/internet/internet-Constitucion-derecho_de_acceso-neutralidad_de_la_red-Ciudadanos_0_451454893.html.

[761] See the introduction of Section 4.1.3. of the current study.

[762] See Section 4.1.3. of the current study.

the basis of the European Union law, and by the ECtHR on the basis of article 10 of the eponymous Convention. That is to say that both courts refer - at least - to the ECHR principles, since freedom of expression is mainly protected in the EU by the EUCFR, which, as mentioned in the introduction of the current study, has the same meaning and scope as the ECHR as regards the right to freedom of expression, even though European Union law may provide more extensive protection. National Courts also generally[763] refer to the ECtHR protection requirements since, as seen previously in our Section 3.2, the ECtHR applies in all the EU Member States.

The protection offered to freedom of expression by the ECtHR is of the same kind as the one offered to private life. Any limitation (such as "*every 'formality', 'condition', 'restriction' or 'penalty' imposed in this sphere*"[764]) must have a legal basis[765], must pursue one of the legitimate aims listed in Article 10§2[766], must be necessary[767] (such necessity being imperatively "*established convincingly*"[768] and must be proportionate to the aim pursued[769]. These conditions "*must be construed strictly*"[770], including in times of crisis[771], keeping in

[763] Where the Constitution or the law does not mention explicitly these general principles, some courts refer to the ECtHR requirements whereas other use own requirements that are adapted to reach the same conclusions as the ECtHR. See our Section 4.3.3.2.

[764] ECtHR, plen., 7 December 1976, *Handyside v. The United Kingdom*, §49, http://hudoc.echr.coe.int/eng?i=001-57499 (Last accessed on 24 May 2017).

[765] ECtHR, ch., 24 September 1992, *Herczegfalvy v. Austria*, appl. n°10533/83, §§91 and 94, http://hudoc.echr.coe.int/eng?i=001-57781; ECtHR, gr.ch., 25 November 1999*, Hashman and Harrup v. the United Kingdo*m, appl. n°25594/94, §§29 *et seq*., http://hudoc.echr.coe.int/eng?i=001-58365; ECtHR, gr. ch., 15 October 2015, *Perinçek v. Switzerland*, appl. n°27510/08, §125, §§131 *et seq* (not. on the principle of foreseeability), http://hudoc.echr.coe.int/eng?i=001-158235 (URLs last accessed on 26 May 2017).

[766] These aims are the interests of national security, territorial integrity or public safety; the prevention of disorder or crime; the protection of health or morals; the protection of the reputation or rights of others; the prevention of the disclosure of information received in confidence; and the maintaining of the authority and impartiality of the judiciary (art. 10 §2). See for ex. ECtHR, *Perinçek v. Switzerland*, *op. cit.* §§141 *et seq.* in relation with the "rights of others".

[767] ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, §50, Series A, n° 30, http://hudoc.echr.coe.int/eng?i=001-57584; ECtHR, plen., 22 May 1990, *Autronic AG v. Switzerland*, appl. n°12726/87, §§61 *et seq*., http://hudoc.echr.coe.int/eng?i=001-57630; See also ECtHR, ch., 29 August 1997, *Worm v. Austria*, appl.n°22714/93, § 47, http://hudoc.echr.coe.int/eng?i=001-58087; ECtHR, ch., 22 May 1990, *Weber v. Switzerland*, appl. n°11034/84, §51 , http://hudoc.echr.coe.int/eng?i=001-57629 (the facts being already known by the public, there was no interest in maintaining their confidentiality and therefore the penalty imposed to the applicant was no necessary); ECtHR, *Handyside v. The United Kingdom, op.cit* §49 on the question to know "*whether 'restrictions' or 'penalties' were conducive to the protection of*" the aim pursued (URLs last accessed on 12 May 2017).

[768] ECtHR, *Perinçek v. Switzerland*, *op. cit.* §196 (i).

[769] ECtHR, *Sunday Times v. The United Kingdom, op cit,* § 63; ECtHR, 25 June 1992, *Thorgeir Thorgeirson v. Iceland*, appl. n°13778/88, §§59 et seq., http://hudoc.echr.coe.int/eng?i=001-57795 (last accessed on 30 May 2017).

[770] ECtHR, gr. ch., 15 October 2015, *Perinçek v. Switzerland*, op. cit. §196 (i).

[771] See for ex. the Council of Europe Committee of Ministers Declaration on freedom of expression and information in the media in the context of the fight against terrorism, 2 March 2005, https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl-02.03.2005&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true (last accessed on 24 May 2017), which especially

mind that freedom of expression "*applies not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb*"[772].

However, the ECtHR has brought some additional clarification to these principles in relation with the protection of freedom of expression specifically.

4.3.3.1.2 Adaptation of the protection requirements to the particularities of freedom of expression

This adaptation of the protection requirements is justified by the specific wording of Article 10§2 and to "*the importance of the rights in question* (...) (which) *has been stressed by the Court many times*"[773].

4.3.3.1.2.1 Duties and responsibilities

Article 10§2 of the ECHR adds that freedom of expression "*carries with it duties and responsibilities*"[774], which refers to the respect that everyone must show for the rights and interests of others, which must be balanced with the freedom of expression[775]. According to the ECtHR; the scope of these duties and responsibilities "*depends on* (...) (the) *situation* (of the person who exercises his or her freedom of expression) *and the technical means he* (or she) *uses*"[776].

This statement highlights firstly the importance of education of citizens to the respect of the rights of others[777], particularly where the freedom of expression is exercised on the Internet since publication is there particularly easy.

---

recommends "*not to introduce any new restrictions on freedom of expression and information in the media unless strictly necessary and proportionate in a democratic society and after examining carefully whether existing laws or other measures are not already sufficient*"; and states that "*the fight against terrorism does not allow the authorities to circumvent this right by going beyond what is permitted by these texts*".

[772] See for ex. ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (i) and the introduction Section 4.3.2.1. of the current report.

[773] ECtHR, *Autronic AG v. Switzerland, op. cit.* §61.

[774] Article 10 §2.

[775] Precautions to be taken by publishers are recalled in several instruments and court decisions. See for ex. the suggestions to media and journalists in the Council of Europe Committee of Ministers Declaration on freedom of expression and information in the media in the context of the fight against terrorism, 2 March 2005, https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl-02.03.2005&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true (last accessed on 24 May 2017); As another example, the Belgium Court of cassation considered that persons at the origin of a publication "*are required to communicate to the public a correct, objective and as exact as possible information. They must refrain from making serious accusations without having verified them sufficiently*" (Translated from Belgian, Decision of 27 April 2007, N° C.06.0123.N, 1.H. R., 2.G. E., contre D. J., p. 3, http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20070427-2 - last accessed on 26 May 2017 - might have to be modified into a pdf file).

[776] ECtHR, *Handyside v. The United Kingdom*, *op. cit.* §49.

[777] See our Section 4.3.2.3.

This statement highlights secondly that the analysis of the context will be of utmost importance in order to determine the degree of legitimacy of the expression, and as a consequence the compliance of the interference with the ECHR requirements.

Indeed, the ECtHR clarifies that States parties to the ECHR "*have a margin of appreciation in assessing whether*"[778] a pressing social need for the limitation does exist, discretion which they must exercise "*reasonably, carefully and in good faith*"[779], but this "*goes hand in hand with European supervision*"[780], during which the ECtHR verifies "*whether the reasons adduced by the national authorities to justify*" the measure "*were relevant and sufficient*", and if "*the interference in the light of the case as a whole* (...) *was proportionate to the legitimate aim pursued*"[781]. As a consequence, the ECtHR is "*empowered to give the final ruling on whether a "restriction" can be reconciled with freedom of expression*"[782].

> In the particular case of a conflict between the protection of the right to freedom of expression and the right to privacy, the ECtHR has "*identified a number of criteria in the context of balancing*" both, which "*must guide its assessment in this area*"[783]. These criteria are the following: "*contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and, where appropriate, the circumstances in which the photographs were taken. Where it examines an application lodged under Article 10, the Court will also examine the way in which the information was obtained and its veracity, and the gravity of the penalty imposed on the journalists or publishers*"[784].

In this context, the ECtHR has brought some clarification in relation to the behaviours that can be limited and to some limitations that cannot be accepted.

4.3.3.1.2.2 Limitation of the right to freedom of expression that can be accepted

The ECtHR considers that certain forms of expression are or might not be admissible, which means that Member States are entitled to prohibit them.

The first one is the "*Denial of the Holocaust and other statements relating to Nazi Crimes*"[785]. The ECtHR generally declares such content inadmissible, considering that such statements are linked to the "*Nazi ideology, which was anti-democratic and inimical to human rights*"[786]. The Court bases its decision either on Article 17[787] of the ECHR where it

[778] ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (ii).

[779] ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (iii).

[780] ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (ii).

[781] ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (iii).

[782] ECtHR, *Perinçek v. Switzerland, op. cit.,* §196 (ii).

[783] ECtHR, gr.ch., 10 November 2015, *Couderc and hachette Filipacchi associés v. France*, appl. n° 40454/07, §93, http://hudoc.echr.coe.int/eng?i=001-158861 (last accessed on 29 May 2017).

[784] *Ibid.*

[785] ECtHR, *Perinçek v. Switzerland, op. cit.,* Section γ before § 209.

[786] ECtHR, *Perinçek v. Switzerland, op. cit.,* § 209.

[787] Which prohibits the abuse of rights.

considers that the complaint is "*incompatible rationae materiae with the provisions of the Convention*"[788], in other words where it considers that the speech does "*negate the fundamental values of the Convention*"[789], or on Article 10 only, considering that the prohibition of the speech was "*necessary in a democratic country*"[790].

The second one is the category of "*calls to violence and 'hate speech'*"[791], in other words of "*statements, verbal or non-verbal, alleged to stir up or to justify violence, hatred or intolerance*"[792]. In these case the Court assesses whether the conditions for limiting freedom to expression have been met, having "*regards to several factors*"[793], knowing that the outcomes of a given case are determined in the light of "*the interplay between the various factors rather than any one of them taken in isolation*"[794], which means that "*the Court's approach to that type of case can thus be described as highly context-specific*"[795]. These factors are especially the following ones:

- The question of "*whether the statements were made against a tense political or social background; the presence of such a background has generally led the Court to accept that some form of interference with such statements was justified*"[796];
- The question of "*whether the statements, fairly construed and seen in their immediate or wider context, could be seen as a direct or indirect call for violence or as a justification of violence, hatred or intolerance.* (...) *In assessing that point, the Court has been particularly sensitive towards sweeping statements attacking or casting in a negative light entire ethnic, religious or other groups*"[797].
- The "*manner in which the statements were made, and their capacity – direct or indirect – to lead to harmful consequences*"[798]. For example statements that "*had been made through poetry rather than in the mass media*" can be protected against interference[799], as well as statements "*made in the course of a deliberately pluralistic televised debate, which had reduced their negative effect*"[800] while statements "*made*

[788] ECtHR, *Perinçek v. Switzerland, op. cit.,* § 212.

[789] ECtHR, Press Unit, Factsheet - Hate speech, February 2012, p.1, http://www.rgsl.edu.lv/uploads/files/ECtHR_fact_Sheet_on_hate_Speech.pdf (last accessed on 29 May 2017).

[790] ECtHR, *Perinçek v. Switzerland, op. cit.,* § 211.

[791] ECtHR, *Perinçek v. Switzerland, op. cit.,* Section β before §204.

[792] ECtHR, *Perinçek v. Switzerland, op. cit.,* §204.

[793] ECtHR, *Perinçek v. Switzerland, op. cit.,* §204.

[794] ECtHR, *Perinçek v. Switzerland, op. cit.,* §208.

[795] ECtHR, *Perinçek v. Switzerland, op. cit.,* §208.

[796] ECtHR, *Perinçek v. Switzerland, op. cit.,* §205.

[797] ECtHR, *Perinçek v. Switzerland, op. cit.,* §206.

[798] ECtHR, *Perinçek v. Switzerland, op. cit.,* §207.

[799] ECtHR, gr.ch., 8 July 1999, *Karataş v. Turkey*, appl. n°23168/94, §§51-52, http://hudoc.echr.coe.int/eng?i=001-58274 (last accessed on 29 May 2017).

[800] ECtHR, 1st Sect., 4 December 2003, *Gündüz v. Turkey*, appl. n°35071/97, §§43-44, http://hudoc.echr.coe.int/eng?i=001-61522 (last accessed on 29 May 2017).

on electoral leaflets", thereby enhancing "*the effect of the discriminatory and hateful message that they were conveying*" might be prohibited[801].[802]

4.3.3.1.2.3 Limitations of the right to freedom of expression that cannot be accepted

On the other hand, the ECtHR identified a series of expressions that can only be narrowly limited or that can even not suffer any restriction unless duly justified overriding requirement in the public interest[803] or in order to maintain the authority of the judiciary[804].

- "***Political expression or (...) debate on questions of public interest*"** are particularly protected against restrictions[805], whereas States "*enjoy a wider margin of appreciation in respect of public morals, decency and religion*"[806].
- "***Prior restraint on freedom of expression*"** are also very narrowly admitted[807].
- **Freedom of expression includes a right to criticism**[808], even if the tone is "*polemical and even aggressive*" ("*the form in which* (ideas) (...) *are conveyed*" being also protected under article 10)[809], as well as "*exaggeration and even provocation*"[810], which is even accepted more broadly where the genre of the publication is "*humorous and satirical (...) as long as the public is not misled about facts*"[811]. In

---

[801] ECtHR, 2nd Sect., 16 July 2009, *Féret v. Belgium*, appl. n°15615/07, §76, http://hudoc.echr.coe.int/eng?i=001-93627 (last accessed on 29 May 2017).

[802] ECtHR, *Perinçek v. Switzerland, op. cit.,* §207.

[803] ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. n°17488/90, §39, http://hudoc.echr.coe.int/eng?i=001-57974 (URL last accessed on 18 May 2017).

[804] ECtHR, plen., 26 November 1991, *Observer and Guardian v. The United Kingdom*, appl. n°13585/88, §68, http://hudoc.echr.coe.int/eng?i=001-57705 (URLs last accessed on 26 May 2017).

[805] ECtHR, *Perinçek v. Switzerland, op. cit.,* §197.

[806] Dr Tarlach McGonagle, The Council of Europe against online hate speech: Conundrums and challenges, expert paper, 2013, p.8, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800c170f (last accessed on 30 May 2017).

[807] ECtHR, gr.ch., 25 November 1999*, Hashman and Harrup v. the United Kingdo*m, appl. n°25594/94, §32, http://hudoc.echr.coe.int/eng?i=001-58365 (last accessed on 26 May 2017); ECtHR, *Observer and Guardian v. The United Kingdom, op. cit.* §59.

[808] ECtHR, plen., 8 July 1986, *Lingens v. Austria*, appl. n°9815/82, §42, http://hudoc.echr.coe.int/eng?i=001-57523 (last accessed on 30 May 2017).

[809] ECtHR, ch., 24 February 1997, *De Haes and Gijsels v. Belgium*, appl. n° 19983/92, §48, http://hudoc.echr.coe.int/eng?i=001-58015 (last accessed on 30 May 2017).

[810] Council of Europe Committee of ministers, Declaration on freedom of political debate in the media, 12 February 2004, available *in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, op. cit.*, p. 282 (quot. p. 283). This quotation refers to ECtHR, ch., 24 February 1997, *De Haes and Gijsels v. Belgium*, appl. n° 19983/92, §46, http://hudoc.echr.coe.int/eng?i=001-58015 and the principle is also mentioned in *Freedom of expression in Europe*, Case-law concerning Article 10 of the European Convention on Human rights, Human Rights files, n°18, Council of Europe publishing, updated ed. March 2007, p 17, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18(2007).pdf (URLs last accessed on 12 May 2017).

[811] Council of Europe Committee of ministers, Declaration on freedom of political debate in the media, *op. cit.*

addition "*the limits of acceptable criticism are* (...) *wider as regards a politician as such than as regards a private individual*"[812], and the Committee of Ministers of the Council of Europe did particularly warn against misuse of defamation legislation including in times of crisis[813]. However, limits do exist and for example the "*harsh criticism of (a) (...) judge's personal and professional integrity was lacking in good faith and not in keeping with the rules of journalistic ethics*"[814].

- **The "*protection of journalistic sources*" is of utmost importance** "*for press freedom in a democratic society*" and as a consequence "*an order of source disclosure (...) cannot be compatible with Article 10 (...) unless it is justified by an overriding requirement in the public interest*", given "*the potentially chilling effect" such an order can have "on the exercise of that freedom*"[815].
- **Article 10 "*protects journalists' rights to divulge information on issues of general interest provided that they are acting in good faith and on an accurate factual basis and provide 'reliable and precise' information in accordance with the ethics of journalism*"[816], even were their source of information has a "*suspect origin*"** since the "*duty and responsibilities*" they have as a result of this suspect origin is overridden by "*the interest in the public's being informed*"[817]. As a consequence, journalists cannot be sentenced for the publication of "*the fruits of a breach of professional confidence*"[818] (in this case Tax documents relating to a company's chairman) where it is done "*in the context of a public debate of general interest*" that goes beyond the data subject[819] and where there is "*no overriding requirement for the information to be protected as confidential*"[820].

---

[812] ECtHR, plen., 8 July 1986, *Lingens v. Austria*, appl. n°9815/82, §42, http://hudoc.echr.coe.int/eng?i=001-57523 (last accessed on 30 May 2017).

[813] Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, *in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society*, Strasbourg, 2016, p. 150, quot. p. 152, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (last accessed on 24 May 2017).p.138 quot. p. 140: "*IV. Guarantees against misuse of defamation legislation: 15. Member states should not misuse in crisis situations libel and defamation legislation and thus limit freedom of expression. In particular, member states should not intimidate media professionals by law suits or disproportionate sanctions in libel and defamation proceedings.16. The relevant authorities should not use otherwise legitimate aims as a pretext to bring libel and defamation suits against media professionals and thus interfere with their freedom of expression*".

[814] *Freedom of expression in Europe*, Case-law concerning Article 10 of the European Convention on Human rights, *op. cit.*, p.16, referring to ECtHR, ch., 26 April 1995, *Prager and Oberschlick v. Austria*, appl. n°15974/90, http://hudoc.echr.coe.int/eng?i=001-57926 (last accessed on 12 May 2017).

[815] All quotations of this paragraph come from ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. n°17488/90, §39, http://hudoc.echr.coe.int/eng?i=001-57974 (URL last accessed on 18 May 2017).

[816] ECtHR, gr.ch., 21 January 1999, *Fressoz and Roire v. France*, appl. n° 29183/95, §54, http://hudoc.echr.coe.int/eng?i=001-58906 (URL last accessed on 18 May 2017).

[817] *Ibid.* §52.

[818] *Ibid.* §22.

[819] *Ibid.* §46.

[820] *Ibid.* §53.

- **"*The punishment of a journalist for assisting in the dissemination of statements made by another person* in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so**" (and the limited nature of a fine is not a relevant argument)[821].
- **Equal treatment between internal and foreign publications is required** and therefore "*the existence of legislation specifically governing publications of foreign origin*"[822] is not admitted, since the right to freedom of expression includes "*freedom to hold opinions and to receive and impart information and ideas without interference (...) and regardless of frontiers*"[823].
- **It is not permitted to not enable persons to escape conviction for defamation *"unless they can prove the truth of their statements"* as regards "*value-judgments*"** since for these latter *"this requirement is impossible of fulfilment"*. Such an impossibility "*infringes freedom of opinion itself, which is a fundamental part"* of the right to freedom of expression.[824] The Court stressed in addition "*the great importance of not discouraging members of the public, for fear of criminal or other sanctions, from voicing their opinions on issues of public concern*"[825].

In addition, the Committee of Ministers of the Council of Europe did express some recommendations and prohibitions directly implied by the provisions of Article 10 of the ECHR. These are the following:

- **"State and private censorship" must be prevented** and to that purpose "*Member states should maintain and enhance legal and practical measures",* while ensuring *"at the same time (...) compliance with the Additional Protocol to the Convention on Cybercrime and other relevant conventions which criminalise acts of a racist and xenophobic nature committed through computer systems. In that context, member states should promote frameworks for self- and co-regulation by private sector actors (such as the ICT industry, Internet service providers, software manufacturers, content providers and the International Chamber of Commerce)"*, which must "ens*ure the protection of freedom of expression and communication"*[826].

---

[821] ECtHR, gr.ch., 23 September 1994, Jersild v. Denmark, appl. n°15890/89, §35, http://hudoc.echr.coe.int/eng?i=001-57891 (URL last accessed on 18 May 2017).

[822] ECtHR, 3rd Sect., 17 July 2001, *Ekin association v. France*, appl. n°39288/98, §62, http://hudoc.echr.coe.int/eng?i=001-59603 (URL last accessed on 18 May 2017).

[823] Article 10§1 of the ECHR.

[824] All quotations come from ECtHR, plen., *Lingens v. Austria, op. cit.* §46.

[825] ECtHR, ch., 22 February 1989, *Barfod v. Denmark*, appl. n°11508/85, §29, http://hudoc.echr.coe.int/eng?i=001-57430 (URL last accessed on 18 May 2017).

[826] Council of Europe, Committee of Ministers, Appendix to the recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet, 7 November 2007, *in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016,* p. 150, quot. p. 152, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (last accessed on 24 May 2017); see also Recommendation CM/Rec(2008)6 on measures to promote the

- **No discrimination must be done between media:** *"In guaranteeing freedom of expression, member states should ensure that national legislation to combat illegal content, for example racism, racial discrimination and child pornography, applies equally to offences committed via ICTs"* [827].

4.3.3.2 Application of the ECtHR protection at domestic levels

In all the EU Member States that have been studied during the MANDOLA project, the requirements of legal basis, legitimate aim, necessity and proportionality apply.

In some countries this is explicitly stated in the Constitution (such as in Greece[828] and in Romania[829]). It might alternatively be considered to be included in the Constitution, such as in Bulgaria[830].

In some other countries this is based on a decision of the Supreme Court (such as in Cyprus[831]) or of the constitutional Council, which directly applies the ECHR requirements

---

respect for freedom of expression and information with regard to Internet filters, 26 March 2008, *pp. 158 et seq.* of the same collection of recommendations.

[827] Council of Europe, Committee of Ministers, Declaration on human rights and the rule of law in the Information Society, *in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016,* p. 288, quot. I.1 p. 289, *op.cit.*

[828] These principles are applicable as requirements for the lawful restriction of freedom of expression on the basis of Art. 25 (1) d of the Constitution: "*Restrictions of any kind which, according to the Constitution, may be imposed upon these rights, should be provided either directly by the Constitution or by statute, should a reservation exist in the latter's favour, and should respect the principle of proportionality*". The above principles apply primarily as regards legislative and administrative acts, which may be subject to judicial control, but also between private persons (Drittwirkung). In particular, Article 25 (1) c of the Constitution provides that "these rights also apply to the relations between individuals to which they are appropriate". Before the constitutional amendment of 2001 which added this provision to the Constitution, case law applied the above principles as general principles of law (See K. Chrysogonos, Civil and Social Rights, 83 et seq).

[829] In article 53 of the Constitution: "*Restriction on the exercise of certain rights or freedoms - (1) The exercise of certain rights or freedoms may only be restricted by law, and only if necessary, as the case may be, for: the defence of national security, of public order, health, or morals, of the citizens' rights and freedoms; conducting a criminal investigation; preventing the consequences of a natural calamity, disaster, or an extremely severe catastrophe. (2) Such restriction shall only be ordered if necessary in a democratic society. The measure shall be proportional to the situation having caused it, applied without discrimination, and without infringing on the existence of such right or freedom*".

[830] According to the MANDOLA legal expert from Bulgaria, on the basis of Art. 57 of the Constitution.

[831] The Supreme Court of Cyprus, which is competent for constitutional and administrative law issues, has applied those principles by following the European Court of Human Right's requirements. More precisely, as it is stated by the doctrine, "*the following main principles govern freedom of expression: (a) freedom is the rule and restriction is the exception; (b) restriction should be provided by law;(c) restriction should be necessary for a constitutionally prescribed legitimate aim; and (d) restriction should be proportional to the legitimate aim pursued within a democratic society*" (C. Stratilatis, A. Emilianides, Media Law, Cyprus, Kluwer Law International, International Encyclopaedia of Laws series., 2015, p. 44). See Cosmos Press Ltd and Another v The Police (1985) 2 CLR 73: "*In the light of the modern trend in interpreting and applying provisions relating to human rights, such as Article 19 of our Constitution and the corresponding article 10 of the European Convention on Human Rights, which forms part of our own Law as well, and in the light of the European Court of Human Rights judgment of "The Sunday Times case", some of which we have quoted in the present judgment, section 122 (b) of Cap. 154, which is a restriction of the right of expression, must be applied in each particular case in a manner as favourable as possible for the freedom of press*". Legal bases used by Constitutional and criminal judges are Art. 12 of the Constitution as regards the principle of legal basis, Art.

(such as in Belgium[832]) or which uses own requirements that are adapted to reach the same conclusions as the ECtHR (such as in Ireland[833], in France[834], in Germany[835] and in Spain[836]).

19(3) of the Constitution on the protection of freedom of expression as regards the principles of legitimate purpose and of necessity, and Article 12(3) of the Constitution as regards the principle of proportionality.

[832] Supreme Court Decision, 27 April 2007, N° C.06.0123.N, 1.H. R., 2.G. E. contre D. J., http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20070427-2 (last accessed on 26 May 2017 - might have to be modified into a pdf file).

[833] In Ireland the case *Cox v. Ireland* (14 [1992] 2 I.R. 503) formed the beginning of the modern use of proportionality in Ireland, considering that law must limit constitutional rights as little as possible, in pursuit of a legitimate purpose. Both in civil and criminal law courts, the judge may assess the compatibility of legislation with the constitution, the Supreme Court rules on these matters. In the Heaney case (Heaney v. Ireland [1994] 3 I.R. 593, §48) the Supreme Court elaborated that the objective of the provision must be of sufficient importance to warrant overriding a constitutionally protected right. It must relate to concerns pressing and substantial in a free and democratic society. The means chosen must pass a proportionality test. They must: (a) be rationally connected to the objective and not be arbitrary, unfair or based on irrational considerations; (b) impair the right as little as possible, and (c) be such that their effects on rights are proportional to the objective.

[834] According to Art. 34 of the Constitution and Art. 4 of the Declaration of Human and Citizen's Rights of 1789, interference with rights guaranteed by the Constitution can only be organised by law. Such a law must be clear, accessible and intelligible (Constitutional Council, Decision n° 2001-455 DC, 12 January 2002, § 9, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2002/2001-455-dc/decision-n-2001-455-dc-du-12-janvier-2002.668.html; Decision n° 2004-503 DC, 12 August 2004, §29, http://www.conseil-constitutionnel.fr/conseil-con..c/decision-n-2004-503-dc-du-12-aout-2004.908.html). The Constitutional Council (CC) also considers that the legislator can limit the exercise of a freedom for a constitutional imperative only (Frédérique Lafay, note under CC, decision n°94-352 DC of 18 January 1995, JCP 95, II, 22 525; Inter alia, the prevention of attempts to public order and offenders prosecution are objectives of constitutional value (CC decision n°94-352 DC, §3, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html). The CC moreover considers that interferences with the exercise of the right to freedom of expression "*must be necessary, adapted and proportionate to the aim pursued*" (CC, Decision n° 2015-512 QPC of 8 January 2016, §5, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2015-512-qpc/decision-n-2015-512-qpc-du-8-janvier-2016.146840.html. The proportionality test it performs is similar to the one performed by the ECtHR, between the general interest on the one hand, and the limitation of a freedom on the other hand, on the basis of the principle of the division of powers (Olivier Dutheillet de Lamothe, "L'influence de la Cour européenne des droits de l'Homme sur le Conseil constitutionnel", 13 February 2009, Conseil constitutionnel, p. 9, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/pdf/Conseil/cedh_130209_odutheillet.pdf (URLs last accessed on 26 May 2017).

[835] The principles of legal basis, of legitimate purpose, of necessity and of proportionality are requirements of any legislative, administrative and judicial act. These principles are derived from the general rule of law in Art. 20 (3) of the Constitution.

[836] As an example, the regulation of freedom of expression can only be made by law (Art. 53 and 161.1b of the Spanish Constitution: Art. 53. 1.: "*The rights and liberties recognised in Chapter Two of the present Title are binding for all public authorities. The exercise of such rights and liberties, which shall be protected in accordance with the provisions of Article 161, 1a), may be regulated only by law which shall, in any case, respect their essential content. 2. Any citizen may assert his or her claim to the protect the liberties and rights recognised in Article 14 and in Section 1 of Chapter Two, by means of a preferential and summary procedure in the ordinary courts and, when appropriate, by submitting an individual appeal for protection («recurso de amparo») to the Constitutional Court. This latter procedure shall be applicable to conscientious objection as recognised in Article 30. 3. The substantive legislation, judicial practice and actions of the public authorities*

In addition, where law does not expressly include the application of these principles in the other legal area than the constitutional one (such as in Ireland[837]), domestic judges refer directly to the ECtHR requirements in their decisions, such as in France[838], in Cyprus[839] and in the Netherlands[840].

However, the way these principles are applied by National Courts may differ[841], "*depending on specific socio-historical context of each State and the degree of protection that the Constitution gives to the fundamental rights and values, resulting in substantial differences in laws, reflected, for example, to different degrees in terms of award of damages and procedural costs, different definitions, different limitations and the reversing of the burden of proof in certain jurisdictions*", as it has been perfectly highlighted by the Romanian Constitutional Court[842].

Such differences of interpretation may be noticed between countries, for example as regards the borders between the right of honour and the right to freedom of

---

shall be based on the recognition, respect and protection of the principles recognised in Chapter Three. The latter may only be invoked in the ordinary courts in the context of the legal provisions by which they are developed"; Art. 161.1.b 1: "The Constitutional Court has jurisdiction over the whole Spanish territory and is competent to hear: individual appeals for protection («recursos de amparo») against violation of the rights and liberties contained in Article 53.2 of the Constitution, in the circumstances and manner to be laid down by law". In addition, the principles of sustainability, exceptionality, need and proportion are included in article 588 bis of the Spanish Criminal Procedure Act that sets the common provisions on intercepting data communications. It requires explicit arguments that justify the need of the measure to implement, as well as the rational indications of criminality evidenced during the investigation previous to the authorisation request of the meddling act.

[837] In Ireland the ECHR and judgements of the ECtHR must be taken into account by national judges on the basis of the European Convention on human rights Act, 2003, http://www.irishstatutebook.ie/eli/2003/act/20/enacted/en/print.html (last accessed on 30 May 2017).

[838] See for ex. Cour de cassation, note explicative, *Liberté d'expression de l'avocat et limites de la critique admissible à l'égard des magistrats agissant dans l'exercice de leurs fonctions (16.12.16)*, https://www.courdecassation.fr/jurisprudence_2/notes_explicatives_7002/avocat_limites_35735.html (last accessed on 30 May 2017).

[839] For example the principle of proportionality in criminal procedure has been applied in Supreme Court, appeal number: 3/2017, Decision of 23 February 2017; Supreme Court CPS Freight Services Ltd v. Attorney General, appeal number 219/2014, 29 February 2016.

[840] The Dutch Constitution addresses this in its articles 93 and 94. The ECHR has a direct effect in so far as it is intended to confer rights to citizens, therefore the ECtHR jurisprudence is followed. Exceptions are assumed in relation to articles 6 and 13. See: HR 18 februari 1986, NJ 1987, 62; HR 30 januari 1996, NJ 1996, 288. According to the constitution, courts and government bodies are bound by treaties and will apply any and all legislation in accordance with international law, including article 10 ECHR. The UN Declaration of human cannot be seen in the same light as the UN Plenary Meeting cannot take binding decisions: HR 23 November 1984, NJ 1985, 604 m.nt. EAA.

[841] Dr Tarlach McGonagle, The Council of Europe against online hate speech: Conundrums and challenges, expert paper, 2013, p.8, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800c170f (last accessed on 30 May 2017).

[842] Decision n°206, 29 April 2013, published in the Official Gazette of Romania, Part I, n°350 of 13 June 2013, with the correction published in the Official Gazette of Romania, Part I, n°380 of 27 June 2013, pp. 3-4, available in English at https://www.ccr.ro/files/products/Decizie_206_2013en.pdf (last accessed on 30 May 2017).

expression[843], even though most countries recognise explicitly the prevalence of the freedom of expression on the right to honour[844].

Such differences of interpretation may also be noticed at a given national level. For example, in Romania, the jurisprudence applying freedom of expression legal protection is sometimes unequal and even hectic. While many court decisions are balanced, some are criticised for infringing basic free speech rights, as judges oblige media outlets and journalists to cover high damage costs, require them to remove online articles for defamatory content or even oblige them to present public excuses[845].

Judges in charge to apply these principles are all the national judges, in all the countries that have been studied.

Legal basis for action in internal law is most of the time the general basis for civil liability (or administrative one where the administration is involved[846]), if the violation of freedom of expression is not invoked at the occasion of another legal dispute implying the act or the law which limits freedom of expression improperly. It is the case in Belgium[847], in Bulgaria[848], in Cyprus[849], in France[850], in Germany[851], in Ireland[852], in the Netherlands[853], in Romania[854], and in Spain[855]. It can however consist of other general provisions, such as in Greece[856].

---

[843] See on this issue the MANDOLA deliverable D2.1 - Definition of illegal hatred and implications, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/.

[844] Such as in Belgium (see Supreme Court, 27 April 2007, N° C.06.0123.N, 1.H. R., *2.G. E. v. D. J.,* http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20070427-2 (last accessed on 26 May 2017 - might have to be modified into a pdf file), p.6), in Cyprus (see for ex. the case *Police v. Ekdotiki Eteria* (1982) 2 C.L.R. 63), in Spain and in the Netherlands.

[845] According to the expert from Romania who has been interviewed.

[846] For example, in France, the general liability of the administration is based on several stable decisions of the Council of State and follows a close approach than the civil liability regime. In Ireland, the European Convention on human rights Act, 2003 organises in its Art. 3 (2) a liability action against the State.

[847] Article 1382 of the civil Code. Moreover the Constitutional judge has ruled that even though the conditions for civil liability are met (which are a fault, a damage and a link between them), there is still an obligation for the judge to balance these conditions with freedom of expression.

[848] Article 45 of the Obligations and Contracts Act -"*Every person must redress the damage he has guiltily caused to another person. In all cases of tort guilt is presumed until proven otherwise*". Everybody can claim before the Bulgarian Court that his/ her freedom of expression has been infringed under art.45 of Obligations and Contracts Act.

[849] The principles of legal basis, of legitimate purpose, of necessity and of proportionality are applied by the civil judge on the basis of ordinary rules on civil liability. In addition, it could theoretically be possible to use Article 19 of the Constitution as the legal basis of a civil liability claim in case of a violation of freedom of expression (but there is no relevant case law yet). Indeed, Cyprus's Supreme Court has established in the landmark case Police v Georgiades (Police v. Georghiades (1983) 2 C.L.R. 33) the possibility to bring a tort action (therefore, a civil liability claim) for an act or omission which violates a right which is protected by the Constitution of the Republic of Cyprus. In that case, Article 15 of the Constitution, which establishes the protection of privacy, was used as a legal basis for a civil liability claim (tort) which is not expressly provided by the Cypriot substantive tort law (Cap 148). This legal axiom has also been affirmed in the case Police v Yiallourou (Police v Yiallourou (1992) 2 Α.Α.Δ. 147), where Article 17 of the Constitution (protection of secrecy of the communications) was used as a legal basis for a tort claim.

[850] Article 1382 of the Civil Code (unless the civil action is based on the law regulating press offences; in this case the legal basis will be this law - see deliverable D2.1 (final) - Definition of illegal hatred and implications,

Indeed, there are very few specific provisions, in domestic laws, subjecting specific infringements to the right to freedom of expression or to certain of its aspects to civil or penal sanctions. The following ones can be however mentioned:

- In a few countries, the prevention of the exercise of freedom of expression might be punished under certain general provisions - even though this remains uncertain - relating to the use of threats or force to cause a person to do, suffer or omit an act (such as in Germany[857], in Cyprus[858] and in Bulgaria[859]).

Section 5, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/.

[851] Section 823 et seq. of the German civil code (BGB). An English version is available at https://www.gesetze-im-internet.de/englisch_bgb/ (last accessed on 30 May 2017).

[852] See for ex. *Irish Law: A student's Guide*, Tort Law, https://lawinireland.wordpress.com/tort-law/ (last accessed on 30 May 2017).

[853] The common civil liability regime is actionable in cases of libel, smear or similar instances of damages to a person reputation, or any other limitation of the freedom of speech. The test employed in the Netherlands attaches relatively low value to reputation and takes into account all circumstances of the case, including the effect, location, damages and other aspects of the illegal act (be that a limiting or actively infringing act).

[854] In addition, Art. 70 of the Civil Code mentions that any person has the right to freedom of expression and that restrictions to this right are possible only under Article 75 of the Civil Code, which specifies that:*"(1) It does not constitute a violation of the rights foreseen in this section the interferences permitted by law or by international conventions and covenants on human rights to which Romania is part of. (2) The exercise of rights and constitutional freedoms in good faith and in compliance with international agreements and conventions to which Romania is part of does not constitute a violation of the rights foreseen in this section*".

[855] On the basis of article 1902 of the Spanish Civil Code: "The person who, as a result of an action or omission, causes damage to another by his fault or negligence shall be obliged to repair the damaged caused". As in the constitutional sphere the violation of a fundamental right leads to compensation, the civil field is focused on financial compensation considered as a reimbursement, as shown in the wording of article 1902 of the Spanish Civil Code. This right of compensation for the damage concerning freedom of expression by civil means is set by the Organic Law of 5 May 1982 of Civil Protection towards honour, personal and family privacy and the right to one's own image.

[856] Any injured person may invoke the right to protection of personality (Article 57 Civil Code) and require any infringement to cease and desist and claim compensation for damages under Article 914 et seq. Civil Code. In particular, Article 57 Section 1 Civil Code states that '*a person who has suffered an unlawful offense on his personality has the right to claim the cessation of such offense as also the non-recurrence thereof in the future'* (This protection includes any aspect of personality, and in particular life, health and corporal integrity, but also honor, dignity, private life and confidentiality, family life, image, voice, written and oral speech, self-determination, religious beliefs, genetic identity, intellectual creations, economic freedom, professional reputation, nationality, etc.: I. Karakostas, Law of Personality, Nomiki Vivliothiki (in Greek, 2012) 90 et seq.; K. Fountedaki, Natural Person and Personality under the Civil Code, Sakkoulas ed. (in Greek, 2012) 148 et seq.). In accordance with Section 3, this is without prejudice to tort liability, i.e., Articles 914 et seq. Furthermore, Article 59 Civil Code provides that in violation of the right to personality moral damages shall be awarded by the courts. For ex., in a case involving the withdrawal of a book from school libraries because of its indecent content, the Athens District Court repealed a previous decision ordering the withdrawal and implemented the right to protection of personality (Art. 57 Civil Code), as it held that the constitutional protection of art prohibits the foreclosure of works of art Single Member Court of Athens 383/2008, DiMEE 2008, 517).

[857] Section 240 of the German penal Code.

[858] Article 91 of the penal Code.

[859] Article 143 of the penal Code.

- In Spain, specific protection measures are provided for in article 20 of the Spanish Constitution. This Article states that any citizen can claim protection of his or her freedom of expression by means of a "*preferential and summary procedure*" before the ordinary courts, and can submit, after the strict fulfilment of the required preconditions, an individual appeal for protection before the Constitutional Court.

4.4 The right to presumption of innocence and related rights

Understanding the right to presumption of innocence and related rights requires addressing the protecting legal instruments of these rights, the notions involved, and the nature and extent of the protection.

4.4.1 Legal instruments protecting the presumption of innocence and related rights

At the international level, the right to presumption of innocence is notably declared by Article 11 of the United Nations Universal Declaration of Human Rights (UDHR), Article 14 of the International Covenant on Civil and Political Rights (ICCPR), and Article 6 of the European Convention on Human Right (ECHR). The two latter instruments protect in addition the right to a fair trial, whereas the latter is protected independently by Article 10 of the UDHR. On the opposite, Article 10 of the UDHR protects the right to not be punished without law, whereas this particular right is declared separately in Article 15 of the ICCPR, and article 7 of the ECHR.

At the European level, the EU Charter of Fundamental rights (EUCFR) protects the right to an effective remedy and to a fair trial in its Article 47, the right to presumption of innocence and the right of defence in its Article 48, and the principles of legality and proportionality of criminal offences and penalties in its Article 49.

The rights to presumption of innocence, to a fair trial and to legality of penal offences are moreover protected in the ten countries that have been studied in the course of the MANDOLA project. However, all these rights are not always protected by the Constitutions. For example, the right to presumption of innocence is not declared in the Constitution in Belgium[860], Greece[861], Germany[862], Ireland[863], and the Netherlands[864]. On the opposite, the

[860] However, pursuant Belgian Supreme Court, presumption of innocence is a generally accepted principle of law (Decision of 24 June 1986, Pas., p.1320; Decision of 17 September 2003, http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20030917-13.

[861] In Greece the principles are however protected on the basis of the ECHR which is regarded as an integral part of the Greek legal order, as it has been ratified by legislative decree 53/1974.

[862] In the German constitution the presumption of innocence is not explicitly mentioned, but the Constitutional Court has determined in several decisions that this principle can be derived from general rule of law (e.g. BVerfGE 74, 358 [370]; 82, 106 [114 f.]) that is reflected in Art. 20 subsec. 3 of the German Constitution.

[863] "*Presumption of innocence is not explicitly stated in the Constitution but it is implicit in the requirement of Article 31.1 that 'no person shall be tried on any criminal charge save in due course of law'. The concept of presumption of innocence is fundamental to the Irish legal system and is (...) the cornerstone of the criminal justice system. An accused person is presumed innocent until proved guilty. The burden of proving this guilt is on the prosecution and it must be proved beyond a reasonable doubt*". In the justice decision DPP v. D O'T (2003), Hardiman J. moreover stated that: "*the presumption of innocence is a vital, constitutionally guaranteed, right of a person accused in a criminal trial and that the right has been expressly recognised in all of the major international human rights instruments currently in force*": Cliodna McAlee, Criminal Law, Fundamental principles and concepts of criminal law,

principle of legality of penal offences lies in the Constitutions of nine countries out of ten, and is declared in the criminal Code in the last one (namely Romania). As regards the right to a fair trial, it is either not always perfectly mentioned in Constitutions and has mainly been included in the domestic systems by application or implementation of the ECtHR jurisprudence.

4.4.2 The notion and the protection of the presumption of innocence

According to the ECtHR, "*the principle of the presumption of innocence requires, inter alia, that when carrying out their duties, the members of a court should not start with the preconceived idea that the accused has committed the offence charged; the burden of proof is on the prosecution, and any doubt should benefit the accused. It is for the prosecution to inform the accused of the case that will be made against him, so that he may prepare and present his defence accordingly, and to adduce evidence sufficient to convict him*"[865].

This principle is applicable in the context of "criminal charges", but the notion of "crime" is autonomous under the jurisprudence of the ECtHR, which means that the criteria used to determine if the criminal area is involved are mainly "*independent of the categorisations employed by the national legal systems of the member States*"[866]. Indeed, in order to determine the criminal nature of the proceeding, the ECtHR retain a set of (not necessarily cumulative) criteria which are the following[867]: the classification in domestic law; the nature of the offence; and the severity of the penalty that the person concerned risks incurring. In evaluating the second of these criteria, some other factors may be considered such as "*whether the legal rule in question is directed solely at a specific group or is of a generally binding character*", "*whether the proceedings are instituted by a public body with statutory powers of enforcement*", "*whether the legal rule has a punitive or deterrent purpose*", "*whether the imposition of any penalty is dependent upon a finding of guilt*", and "*how comparable procedures are classified in other Council of Europe member States*"[868].

This being said, "*a person's right in a criminal case to be presumed innocent and to require the prosecution to bear the onus of proving the allegations against him or her is not*

---

https://www.ibat.ie/downloads/Sample_notes/Legal%20Studies/Criminal%20Law%20-%20Cliodna%20McAlee.pdf, p. 2, (last accessed on 7 June 2017).

[864] The presumption of innocence is however "*considered to be a fundamental principle of criminal law*": Anne Ruth Mackor and Vincent Geeraets, *The Presumption of Innocence*, Netherlands Journal of Legal Philosophy 2013 (42) 3, http://www.bjutijdschriften.nl/tijdschrift/rechtsfilosofieentheorie/2013/3/NJLP_2213-0713_2013_042_003_001 (last accessed on 7 June 2017).

[865] ECtHR, *Guide on Article 6 of the European Convention on Human rights, Right to a fair trial*, Council of Europe/European Court of Human Rights, 2014, p. 36, http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf, referring for ex. to ECtHR, plen., 6 December 1988, *Barberà, Messegué and Jabardo v. Spain*, appl. n°10590/83, § 77, http://hudoc.echr.coe.int/eng?i=001-57429 (URLs last accessed on 2 June 2017).

[866] *Ibid.,* p. 7, referring to ECtHR, ch., 26 March 1982, *Adolph v. Austria*, appl. n°8269/78, § 30, http://hudoc.echr.coe.int/eng?i=001-67305 (last accessed on 2 June 2017).

[867] Outlined in ECtHR, plen., 8 June 1976, *Engel and Others v. the Netherlands*, appl. n°s 5100/71 5101/71 5102/71 (...), §§ 82-83, http://hudoc.echr.coe.int/eng?i=001-57479 (last accessed on 2 June 2017); see ECtHR, *Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, op. cit.* p.8.

[868] ECtHR, *Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, op. cit.* p.8.

absolute". Indeed, "*presumptions of fact or of law*", which "*operate in every criminal-law system (...) (are) not prohibited in principle by the Convention*"[869]. In particular, Member States may "*under certain conditions, penalise a simple or objective fact as such, irrespective of whether it results from criminal intent or from negligence*"[870]. However, States must "confine these presumptions within reasonable limits which take into account the importance of what is at stake and maintain the rights of the defence"[871].

Indeed, the right to presumption of innocence is, under Article 6 ECHR, one of the requirements of the more general right to a fair trial.

4.4.3 The notion and the protection of the right to a fair trial

The right to a fair trial includes several sub-rights which are mainly the right to access to a court, the right to benefit from several institutional and procedural guarantees (tribunal established by law, independent and impartial; fairness, equality of arms and adversarial proceedings; reasoning of judicial decisions; right to remain silent and to not incriminate oneself; use of evidence obtained lawfully; right to a public hearing and to be judged within a reasonable timeframe), and the right to benefit from a set of specific guarantees amongst which lie the presumption of innocence and the rights of the defence[872].

The Council of Europe Committee of Ministers recalled that the rights to a fair trial and to the presumption of innocence "*should be respected in the digital environment*"[873]

4.4.4 The notion and the protection of the principle of legality of penal offences

This principle, according to which "*only the law can define a crime and prescribe a penalty*"[874] (which implies the principle of non-retroactivity of criminal law, except for lighter penalties[875]), applies to the autonomous notion of "criminal area" as it has been defined in relation to the right to presumption of innocence[876]. The concept of "law" is in addition understood broadly, as in the other ECHR provisions, and covers "*both domestic legislation and case-law, and comprises qualitative requirements, notably those of accessibility and*

---

[869] *Ibid.,* p. 36, referring to ECtHR, 2nd Sect., 19 October 2004, *Falk v. the Netherlands*, appl. n°66273/01, § 77, http://hudoc.echr.coe.int/eng?i=001-67305 (last accessed on 2 June 2017).

[870] *Ibid.,* p. 36, referring for ex. to ECtHR, ch., 7 December 1988, *Salabiaku v. France*, appl. n°10519/83, § 27; http://hudoc.echr.coe.int/eng?i=001-57570 (last accessed on 2 June 2017).

[871] *Ibid.,* p. 36, referring for ex. to ECtHR, *Salabiaku v. France, op. cit.* § 28.

[872] ECtHR, *Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, op. cit.* pp.11-55.

[873] Appendix to the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, 7 November 2007, I (Human Rights and democracy), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008_CMrec0711_en.PDF (last accessed on 31 May 2017).

[874] ECtHR, *Guide on Article 7 of the European Convention on Human Rights, No punishment without law: the principle that only the law can define a crime and prescribe a penalty*, updated 30 April 2017, Council of Europe/European Court of Human Rights, 2017, http://www.echr.coe.int/Documents/Guide_Art_7_ENG.pdf (last accessed on 31 May 2017).

[875] ECtHR, *Guide on Article 7 of the European Convention on Human Rights, op. cit.,* pp. 16, 18.

[876] ECtHR, *Guide on Article 7 of the European Convention on Human Rights, op. cit.,* p.6. See Section 4.4.2. of the current study.

foreseeability"[877]. The concept of penalty has also an autonomous scope and the ECtHR is "*free to go beyond appearances*". It "*autonomously assess*(es) *whether a specific measure is, substantively, a 'penalty' within the meaning of Article 7 § 1. The starting point for any assessment of the existence of a 'penalty' is to ascertain whether the measure in question was ordered following a conviction for a 'criminal offence'. Other factors may be deemed relevant in this respect: the nature and aim of the measure in question (particularly its punitive aim), its classification under domestic law, the procedures linked to its adoption and execution and its severity (...). However, the severity of the measure is not decisive in itself, because many non-criminal measures of a preventive nature can have a substantial impact on the person concerned*"[878].

According to the Council of Europe Committee of Ministers, and as well as the right to a fair trial, "*the right of no of no punishment without law applies equally to a digital and a non-digital environment*" [879].

4.5 The right to be protected against discrimination

Understanding the right to be protected against discrimination requires addressing the protecting legal instruments of this right, the notion of discrimination in this context, and the nature and extent of its protection.

4.5.1 Legal instruments protecting the right to right to non-discrimination

As well as the other rights studied in this report, the right to non-discrimination is protected on one hand by International and European texts, and on the other hand by national constitutions and laws.

4.5.1.1 International and European instruments

At the international level, the right to non-discrimination is notably declared by Article 7 of the United Nations Universal Declaration of Human Rights, Article 26 of the International Covenant on Civil and Political Rights, and by the UN International Convention on the elimination of all forms of racial discrimination.

At the Council of Europe level more specifically, the prohibition of discrimination is declared in Article 14 of the ECHR, which prohibits discrimination when applying the other provisions of the Convention, and in the additional protocol n°12 to the ECHR, which provides for a general prohibition of discrimination. Such prohibition is also partly regulated by the Council of Europe additional protocol (of 28 January 2003) to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

At the European Union level, it is protected by Article 21 of the EU Charter of Fundamental rights (EUCFR) and by several more specific instruments including the Council Directive

[877] ECtHR, *Guide on Article 7 of the European Convention on Human Rights, op. cit.,* p.6.

[878] ECtHR, *Guide on Article 7 of the European Convention on Human Rights, op. cit.,* p.7.

[879] Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, I.5, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp (URLs last accessed on 31 May 2017).

2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin and the Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services. The prohibition of discrimination is moreover partly regulated in the Council Framework Decision 2008/913/JHA of November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.[880]

In the same way as for other fundamental rights studied in the current report, the Council of Europe and EU systems are complementary and can be interchangeable sources within the framework of an analysis of the notion of discrimination and of its protection, even though minor differences can be highlighted[881].

4.5.1.2 National Constitutions

The right to non-discrimination is moreover protected by several national Constitutions, and by all the countries that have been studied in the course of the MANDOLA project.

In Belgium, the prohibition of discrimination is declared in Articles 10, 11, 11bis and 131[882] of the Constitution.

In Bulgaria, the prohibition of discrimination is declared in Article 6 of the Constitution[883].

In Cyprus, the prohibition of discrimination is declared in Article 28 of the Constitution[884].

In France, the prohibition of discrimination is declared in Article 1 of the Declaration of Human and Citizen's Rights of 1789[885], which belongs to the French "Constitutional bloc".

---

[880] For an extensive list of applicable instruments see *Handbook on European non-discrimination law*, European Union Agency for Fundamental Rights / Council of Europe / European Court of Human Rights, 2010, p. 145, http://fra.europa.eu/sites/default/files/fra_uploads/1510-FRA-CASE-LAW-HANDBOOK_EN.pdf (last accessed on 31 May 2017).

[881] *Handbook on European non-discrimination law*, 2010, *op. cit*., back cover.

[882] **Article 10:** "*There shall be no distinction between orders in the State. Belgians are equal before the law; they alone shall be eligible for civil and military service, save as may be otherwise provided by law in particular cases. Equality between genders is guaranteed*". **Article 11:** "*The enjoyment of the rights and freedoms accorded to Belgians shall be secured without discrimination. To this end, the law and decrees especially guarantee the rights and freedoms of ideological and philosophical minorities*". **Article 11bis:** "*Law, decree and norms referred to in Article 134 guarantee to women and men the equal exercise of their rights and freedoms, and especially favour their equal access to elective and public office*". **Article 131:** "*The law determines the measures in order to prevent any discrimination based on ideological or philosophical grounds*".

[883] **Article 6 (1):** *"All persons are born free and equal in dignity and rights".* **(2):** *"All citizens shall be equal before the law. Neither abridgement of rights nor any privileges whatsoever shall be admissible on the basis of race, nationality, ethnic identity, sex, origin, religion, education, convictions, political affiliation, personal and social status, or property status"*.

[884] **Article 28 (1):** *"[A]ll persons are equal before the law, the administration, and justice, and are entitled to equal protection thereof and treatment thereby".* **Article 28 (2):** *"Every person shall enjoy all the rights and liberties provided for in this Constitution without any direct or indirect discrimination against any person on the ground of his community, race, religion, language, sex, political or other convictions, national or social descent, birth, colour, wealth, social class, or on any ground whatsoever, unless there is express provision to the contrary in this Constitution*".

In Germany, the prohibition of discrimination is declared in Article 3 of the Constitution *('Grundgesetz')*[886].

In Greece, the prohibition of discrimination is declared in Article 5 (2) of the Constitution[887].

In Ireland, the prohibition of discrimination is declared in Article 40 of the Constitution[888].

In the Netherlands, the prohibition of discrimination is declared in Article 1 of the Constitution[889].

In Romania, the prohibition of discrimination is declared in Articles 16 and 20 of the Constitution[890].

In Spain, the prohibition of discrimination is declared in article 14 of the Constitution[891].

4.5.2 The notion of discrimination

According to the ECtHR and the European Union agency for fundamental rights, "*the aim of non-discrimination law is to allow all individuals an equal and fair prospect to access opportunities available in a society*"[892]. This implies two requirements, namely the absence of direct and indirect discrimination.

- **Absence of direct discrimination:** the first requirement is that "*those individuals who are in similar situations should receive similar treatment and not be treated less favourably simply because of a particular 'protected' characteristic that they possess". This is known as 'direct' discrimination. Direct discrimination, if framed under the ECHR, is subject to a general objective justification defence; however, under EU law defences against direct discrimination are somewhat limited*"[893].

---

[885] **Article 1:** "*Men are born and remain free and equal in rights. Social distinctions may be based only on considerations of the common good*".

[886] **Article 3 - Equality before the law: (1)** "*All persons shall be equal before the law*". **(2)** "*Men and women shall have equal rights. The state shall promote the actual implementation of equal rights for women and men and take steps to eliminate disadvantages that now exist*". **(3)** "*No person shall be favoured or disfavoured because of sex, parentage, race, language, homeland and origin, faith, or religious or political opinions. No person shall be disfavoured because of disability*".

[887] **Article 5 (2):** "*all persons living within the Greek territory shall enjoy full protection of their life, honour and liberty irrespective of nationality, race or language and of religious or political beliefs. Exceptions shall be permitted only in cases provided by international law*".

[888] **Article 40.6. 1°**"*The State guarantees liberty for the exercise of the following rights, subject to public order and morality: i The right of the citizens to express freely their convictions and opinions* (...)".

[889] **Article 1:** "*All persons in the Netherlands shall be treated equally in equal circumstances. Discrimination on the grounds of religion, belief, political opinion, race or sex or on any other ground whatsoever shall not be permitted*".

[890] **Article 16 – Equality of rights:** *"(1) Citizens are equal before the law and public authorities, without any privilege or discrimination".* **Article 20 – International Treaties on Human Rights:** *"(1) Constitutional provisions concerning the citizens' rights and liberties shall be interpreted and enforced in conformity with the Universal Declaration of Human Rights, with the covenants and other treaties Romania is a party to".*

[891] **Article 14:** "*Spaniards are equal before the law and may not in any way be discriminated against on account of birth, race, sex, religion, opinion or any other personal or social condition or circumstance".*

[892] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 21.

[893] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 21.

- **Absence of indirect discrimination:** the second requirement is that "*those individuals who are in different situations should receive different treatment to the extent that this is needed to allow them to enjoy particular opportunities on the same basis as others. Thus, those same 'protected grounds' should be taken into account when carrying out particular practices or creating particular rules. This is known as 'indirect' discrimination. All forms of indirect discrimination are subject to a defence based on objective justification irrespective of whether the claim is based on the ECHR or EU law*"[894].

Direct discrimination occurs in the following situation:

- "*an individual is treated unfavourably,*
- *by comparison to how others, who are in a similar situation, have been or would be treated,*
- *and the reason for this is a particular characteristic they hold, which falls under a 'protected ground'"*[895] or *"to another factor that is indissociable from the protected ground*" (for example, the fact to be retired or not, if at an identical age retirement legally depends on the gender[896]).

  Protected grounds shared without any doubts at the EU and ECHR level are the following: sex, sexual orientation, disability, age, race, ethnicity or ethnic origin, nationality or national origin, religion or belief[897].

  Additional grounds protected by the ECtHR (which might also be in certain cases protected indirectly by EU law) are the following: colour and membership of a national minority, language, social origin, birth and property, political or other opinion, and a set of "other values" that encompasses disability, age, and sexual orientation, fatherhood, marital status, membership of an organisation, military rank, parenthood of a child born out of wedlock, place of residence[898], health including HIV infection[899].

One manifestation of direct discrimination is harassment and instruction to discriminate, which are specifically protected by EU directives[900]. At the Council of Europe level, harassment "*may fall under the right to respect for private and family life protected under Article 8 of the ECHR, or the right to be free from inhuman or degrading treatment or punishment under Article 3, while instruction to discriminate may be caught by other*

[894] *Handbook on European non-discrimination law*, 2010, *op. cit*., pp. 21-22.

[895] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 22.

[896] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 26.

[897] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 26 and pp. 89 *et seq*.

[898] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 26 and pp. 89 *et seq*.

[899] *Handbook on European non-discrimination law: Case-law update July 2010-December 2011*, European Union Agency for Fundamental Rights / Council of Europe / European Court of Human Rights, 2012 http://www.echr.coe.int/Documents/Handbook_non_discri_law_ENG_02.pdf (last accessed on 31 May 2017).

[900] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 31.

Articles, such as freedom of religion or assembly under Article 9 or 11, depending on the context" [901].

Indirect discrimination appears where:

- "*a neutral rule, criterion or practice*
- *affects a group defined by a 'protected ground' in a significantly more negative way*
- *by comparison to others in a similar situation*" [902].

4.5.3 Nature and extent of right to be protected against discriminations

The protection against discrimination applies in relation to different areas depending on legal instruments that base the action.

4.5.3.1 Nature of the protection against discrimination

Discrimination is prohibited and are only admitted, in particular circumstances, "*defences of less favourable treatments*"[903].

The ECtHR operates "*a generally phrased defence*", which applies in the context of both direct and indirect discrimination under the ECHR, and which applies in the context of indirect discrimination only under EU law[904]. This general defence is the following:

"*In order for an issue to arise under Article 14 there must be a difference in the treatment of persons in relevantly similar situations (...). Such a difference of treatment is discriminatory if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised. The Contracting State enjoys a margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a different treatment, and this margin is usually wide when it comes to general measures of economic or social strategy*"[905].

Under EU law in the context of direct discrimination, only "*a specific set of defences*" does exist "*allowing differential treatment to be justified in a limited set of circumstances*"[906]. They are interpreted "narrowly" by the EUCJ which emphasis, in its jurisprudence, "on the importance of any rights created for individuals under EU law"[907].

- The first one is the "*genuine occupational requirement defence*", which "*allows employers to differentiate against individuals on the basis of a protected ground*

[901] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 34.

[902] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 29.

[903] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 43.

[904] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 43.

[905] See ECtHR, gr. ch., 29 April 2008, *Burden v. the United Kingdom*, appl. 13378/05, §60, http://hudoc.echr.coe.int/eng?i=001-86146 (last accessed on 7 June 2017), *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 44.

[906] *Handbook on European non-discrimination law*, 2010, *op. cit*., pp. 45-46.

[907] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 46.

where this ground has an inherent link with the capacity to perform or the qualifications required of a particular job"[908].

- The second one is the "the permissibility of discrimination on the basis of religion or belief by employers who are faith-based organisations"[909].
- The third one is the permissibility of age discrimination in certain circumstances[910].

4.5.3.2 Extent of the protection against discrimination

The scope of the protection is different depending on the legal instrument taken as a basis to ensure it.

The ECHR protects against discrimination "*in relation to the enjoyment of the substantive rights guaranteed by the ECHR*"[911]. In addition, Protocol 12 to the ECHR "*expands the scope of the prohibition on discrimination to cover any right which is guaranteed at the national level, even where this does not fall within the scope of an ECHR right*"[912]. However, this Protocol is in force in only 20 of the 47 members of the Council of Europe[913], among which 10 are EU Member States. "*This means that among the EU Member States there exist different levels of obligations in European non-discrimination law*"[914].

The EU law prohibits direct and indirect discrimination in some particular spheres only, namely employment, access to welfare and forms of social security, access to education, access to supply of goods and services including housing and access to justice[915].

4.6 The right to freedom of assembly

Understanding the right to freedom of assembly requires addressing the protecting legal instruments of this right, the notion of freedom of assembly, and the nature and extent of its protection.

4.6.1 Legal instruments protecting the freedom of assembly

At the international level, the right to freedom of assembly is notably declared by Article 20 of the United Nations Universal Declaration of Human Rights, Article 21 of the International Covenant on Civil and Political Rights, and Article 11 of the European Convention on Human Right (ECHR). At the European level, it is protected by Article 12 of the EU Charter of Fundamental rights (EUCFR).

---

[908] *Ibid.*

[909] *Ibid.*

[910] *Ibid.*

[911] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 57.

[912] *Ibid.*

[913] Council of Europe, Chart of signatures and ratifications of Treaty 177, Status as of 07/06/2017 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/177/signatures?p_auth=vPBoLvM0.

[914] *Handbook on European non-discrimination law*, 2010, *op. cit*., p. 57.

[915] *Handbook on European non-discrimination law*, 2010, *op. cit*., pp. 57 *et seq*.

4.6.2 The notion of freedom of assembly

Freedom of assembly "*includes public or private meetings, marches, processions, demonstrations and sit-ins. The purpose may be political, religious or spiritual, social or another purpose; no limit has been imposed on purpose, but any assembly must be peaceful. Incidental violence will not mean an assembly forfeits protection unless it had a disruptive purpose*"[916].

Freedom of assembly has an "*autonomous role and particular sphere of application*"[917]. However, one of its objectives is "*the protection of personal opinions, secured by Article 10*"[918]. Accordingly, it must in certain situations "*be considered in the light of Article 10*" [919].

According to the Council of Europe Committee of Ministers, freedom of Assembly also implies that "*individuals are free to use Internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards*". In the same line, according to the Committee of Ministers, "*individuals* (should be) (...) *free to use Internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly*"[920].

Indeed, "*ICTs bring an additional dimension to the exercise of freedom of assembly and association, thus extending and enriching ways of enjoying these rights in a digital environment. This has crucial implications for the strengthening of civil society, for participation in the associative life at work (trade unions and professional bodies) and in the political sphere, and for the democratic process in general*" [921]. For this purpose, the Council of Europe Committee of Ministers recommends that Member States "*adapt their legal frameworks to guarantee freedom of ICT-assisted assembly and take the steps necessary to ensure that monitoring and surveillance of assembly and association in a digital environment*

[916] Council of Europe, *Freedom of assembly and association*, http://www.coe.int/en/web/echr-toolkit/la-liberte-de-reunion-et-dassociation (last accessed on 31 May 2017).

[917] See for ex. ECtHR, gr.ch., 26 September 1995, *Vogt v. Germany*, appl. 17851/91, §64, http://hudoc.echr.coe.int/eng?i=001-58012 (last accessed on 31 May 2017).

[918] *Ibid.*

[919] *Ibid.*

[920] Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, n°3, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa; See also Appendix to the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, 7 November 2007, I (Human Rights and democracy), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008_CMrec0711_en.PDF; Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp (URLs last accessed on 31 May 2017).

[921] Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, op. cit., n°8 (Freedom of assembly).

does not take place, and that any exceptions to this must comply with those provided for in Article 11, paragraph 2, of the ECHR"[922].

4.6.3 Nature and extent of the freedom of assembly protection

In the same way as for other conditional fundamental rights[923], the protection of the freedom of assembly implies for contracting States to not interfere arbitrarily with this freedom, and also implies for these States the positive obligation to secure the exercise of it[924], which means to "*take reasonable and appropriate measures to enable lawful demonstrations to proceed peacefully*"[925], particularly in order "*to prevent violent acts directed against the participants*"[926] in the exercise of the right, taking the specific circumstances into account[927], and particularly where is concerned the freedom of assembly and association of "*persons belonging to minorities, including national and ethnic minorities*"[928].

This positive obligation does not mean that freedom of association is absolute[929], since States have also the positive obligation to secure the other rights and freedom, and it can for example not "*be accepted that (...) an association, through its activities or the intentions it has expressly or implicitly declared in its programme, jeopardises the State's institutions or the rights and freedoms of others*"[930]. In such case, States are authorised to limit freedom of assembly in order "*to protect those institutions and persons*" [931].

Any interference requires justification under Article 11 § 2 of the ECHR, and must accordingly - in the same way as for other conditional fundamental rights[932] - "*be (i)*

[922] *Ibid.*

[923] See especially Sections 4.1.3 and 4.2.3 of the current report.

[924] ECtHR gr. ch., 17 February 2007, *Gorzelik and others v. Poland*, appl. n°44158/98, §94, http://hudoc.echr.coe.int/eng?i=001-61637 (last accessed on 31 May 2017).

[925] ECtHR, 1st Sect., 20 October 2005, The United Macedonian Organisation Ilinden and Ivanov v. Bulgaria, appl. n°44079/98, §115, http://hudoc.echr.coe.int/eng?i=001-70678 (last accessed on 31 May 2017).

[926] *Ibid.* §115. See also Council of Europe, *Freedom of assembly and association*, *op. cit.*

[927] *Ibid.* §115.

[928] ECtHR, *Gorzelik and others v. Poland, op. cit.* §93: "*The Court recognises that freedom of association is particularly important for persons belonging to minorities, including national and ethnic minorities, and that, as laid down in the preamble to the Council of Europe Framework Convention, ' pluralist and genuinely democratic society should not only respect the ethnic, cultural, linguistic and religious identity of each person belonging to a national minority, but also create appropriate conditions enabling them to express, preserve and develop this identity' . Indeed, forming an association in order to express and promote its identity may be instrumental in helping a minority to preserve and uphold its rights*". Cee also §90: "*democracy does not simply mean that the views of the majority must always prevail: a balance must be achieved which ensures the fair and proper treatment of minorities and avoids any abuse of a dominant position*".

[929] ECtHR, *Gorzelik and others v. Poland, op. cit.* §94.

[930] *Ibid.* §94.

[931] *Ibid.* §94.

[932] See Section 4.1.3. of the current report.

prescribed by law (ii) for a permitted purpose[933]*"*[934], (iii) necessary in a democratic society and (iv)proportionate to the legitimate aim pursued[935], which might also be assessed in conjunction with Article 14 of the ECHR, and implies as a consequence that restrictions of the freedom of assembly "*are non-discriminatory*"[936], in other words that they do not "*create a difference in treatment between persons in comparable situations*"[937].

The ECtHR clarifies that the power of interference must "*be used sparingly, as exceptions to the rule of freedom of association are to be construed strictly and only convincing and compelling reasons can justify restrictions on that freedom*"[938].

The Court also clarifies the nature of its assessment:

> "*It is in the first place for the national authorities to assess whether there is a "pressing social need" to impose a given restriction in the general interest. While the Convention leaves to those authorities a margin of appreciation in this connection, their assessment is subject to supervision by the Court, going both to the law and to the decisions applying it, including decisions given by independent courts*".
>
> "*When the Court carries out its scrutiny, its task is not to substitute its own view for that of the national authorities, which are better placed than an international court to decide both on legislative policy and measures of implementation, but to review under Article 11 the decisions they delivered in the exercise of their discretion. This does not mean that it has to confine itself to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith; it must look at the interference complained of in the light of the case as a whole*[939] *and determine whether it was "proportionate to the legitimate aim pursued" and whether the reasons adduced by the national authorities to justify it are "relevant and sufficient". In so doing, the Court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 11 and, moreover, that they based their decisions on an acceptable assessment of the relevant facts*" [940].
>
> Especially, where a threat is invoked by a given State as a justification for the interference, the ECtHR verifies, "*that the risk alleged is real and substantial and that the impugned interference with freedom of association does not go beyond what is necessary*

---

[933] According to Art. 11§2, permitted purposes are national security or public safety, 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.

[934] Council of Europe, *Freedom of assembly and association*, *op. cit.*

[935] Art. 11§2 of the CEDH. See also Council of Europe, *Freedom of assembly and association*, *op. cit.* For an application see for ex. ECtHR, *Gorzelik and others v. Poland, op. cit.* §§ 64, 76, 77 *et seq*.

[936] Council of Europe, *Freedom of assembly and association*, *op. cit.*

[937] ECtHR, gr.ch., 29 April 1999, *Chassagnou and others v. France*, appl. n°s 25088/94, 28331/95, 28443/95, §120, http://hudoc.echr.coe.int/eng?i=001-58288 (last accessed on 31 May 2017).

[938] ECtHR, *Gorzelik and others v. Poland, op. cit.* §95.

[939] And in the light of the circumstances of this particular case: ECtHR, *Gorzelik and others v. Poland, op. cit.* §105; ECHR, gr. ch., 9 July 2013, *Sindicatul "Păstorul cel Bun" v. Romania*, appl. 2330/09, § 159, http://hudoc.echr.coe.int/eng?i=001-122763 (last accessed on 31 May 2017).

[940] ECtHR, *Gorzelik and others v. Poland, op. cit.* §96.

to eliminate that risk and does not serve any other purpose unrelated to the exercise of the religious community's autonomy" [941].

Regarding more particularly "*State measures applied in the context of the exercise of the right to peaceful assembly which amount to a blocking or restriction of Internet platforms*"[942], the Council of Europe Committee of Ministers recalls the requirements of legal basis, legitimate aim, necessity and proportionality as well as their meaning, highlighting particularly that there must be "*a fair balance between the exercise of the right to freedom of assembly and freedom of association and the interests of the society as a whole. If a less intrusive measure achieves the same goal, it is applied. The restriction is narrowly construed and applied, and does not encroach on the essence of the right to freedom of assembly and association*"[943]

Finally, the ECtHR explains that "*the boundaries between the State's positive and negative obligations under Article 11 of the Convention do not lend themselves to precise definition. The applicable principles are nonetheless similar. Whether the case is analysed in terms of a positive duty on the State or in terms of interference by the public authorities which needs to be justified, the criteria to be applied do not differ in substance. In both contexts regard must be had to the fair balance to be struck between the competing interests of the individual and of the community as a whole*"[944].

4.7 The right to freedom of movement

Understanding the right to freedom of movement requires addressing the protecting legal instruments of this right, the notion of freedom of movement, and the nature and extent of its protection.

4.7.1 Legal instruments protecting the freedom of movement

At the international level, the right to freedom of movement is notably declared by Article 12 of the United Nations Universal Declaration of Human Rights, Article 12 of the International Covenant on Civil and Political Rights and Article 2 of the Protocol n°4[945] to the European Convention on Human Right (ECHR). At the European level, it is protected by Article 45 of the EU Charter of Fundamental rights (EUCFR) and by Article 11 of the Community Charter of the Fundamental Social Rights of Workers.

[941] ECHR, gr. ch., 9 July 2013, *Sindicatul "Păstorul cel Bun" v. Romania*, appl. 2330/09, § 159, http://hudoc.echr.coe.int/eng?i=001-122763 (last accessed on 31 May 2017).

[942] Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, op. cit., Section 3.4.

[943] *Ibid.,* Section 3.5.

[944] ECHR, gr. ch., 9 July 2013, *Sindicatul "Păstorul cel Bun" v. Romania*, appl. 2330/09, § 132, http://hudoc.echr.coe.int/eng?i=001-122763 (last accessed on 31 May 2017).

[945] Protocol n°4 securing certain rights and freedoms other than those already included in the Convention and in the First Protocol thereto, 16 September 1963.

4.7.2 The notion of freedom of movement

Article 2 of Protocol No. 4 "*guarantees to any person a right to liberty of movement within a given territory and the right to leave that territory, which implies the right to travel to a country of the person's choice to which he or she may be admitted*"[946]. The "*freedom to choose one's residence*" is protected under this freedom, and more precisely "*is at the heart of Article 2 § 1 of Protocol No. 4, which provision would be voided of all significance if it did not in principle require Contracting States to accommodate individual preferences in the matter*"[947].

4.7.3 Nature and extent of the freedom of movement protection

According to the Court's case-law, "*any measure restricting the right to liberty of movement must be in accordance with law, pursue one of the legitimate aims referred to in the third paragraph of Article 2 of Protocol No. 4 and strike a fair balance between the public interest and the individual's rights*".[948]

The test applied by the ECtHR is the same as the one applied in order to assess interferences with the right to privacy, studied in Section 4.1.3 of the current report[949].

4.8 The right to liberty and security

Understanding the right to liberty and security requires addressing the protecting legal instruments of this right, the notion of "liberty and security" in this context, and the nature and extent of its protection.

4.8.1 Legal instruments protecting the right to liberty and security

At the international level, the right to liberty and security is notably declared by Article 3 of the United Nations Universal Declaration of Human Rights, Article 9 of the International Covenant on Civil and Political Rights, Article 5 of the ECHR and Article 1 of the Protocol n°4[950] to the ECHR). At the European level, it is protected by article 6 of the EUCFR).

4.8.2 The notion of right to liberty and security

The right to liberty and security refers to the "*physical liberty*" of the person, ensuring that no one is "*deprived of that liberty in an arbitrary fashion*"[951]. It is a "*unique right, as the*

---

[946] ECtHR, gr. ch., 23 February 2017, *De Tommaso v. Italy*, appl. n°43395/09, §104, http://hudoc.echr.coe.int/eng?i=001-171804 (last accessed on 31 May 2017).

[947] ECtHR, 3rd Sect., 23 February 2016, *Garib v. The Netherlands*, appl. n° 43494/09, §115, http://hudoc.echr.coe.int/eng?i=001-161054 (last accessed on 31 May 2017).

[948] ECtHR, *De Tommaso v. Italy*, op. cit. §104.

[949] ECtHR, *De Tommaso v. Italy*, *op. cit.* §§106-109; ECtHR, *Garib v. The Netherlands*, *op. cit.* §§105 *et seq*.

[950] Protocol n°4 securing certain rights and freedoms other than those already included in the Convention and in the First Protocol thereto, 16 September 1963.

[951] ECtHR, Guide on Article 5 of the Convention, Right to liberty and security, Council of Europe/European Court of Human Rights, 2014, p.5, http://www.echr.coe.int/Documents/Guide_Art_5_ENG.pdf (last accessed on 31 May 2017).

expression has to be read as a whole"[952]*.* The notion of "*Security of a person serves to underline a requirement that the authorities in Strasbourg have developed when interpreting and explaining the right to liberty in Article 5"* [953], and it "*must be understood in the context of physical liberty and it cannot be interpreted as to referring to different matters (such as a duty on the state to give someone personal protection form an attack by others, or right to social security)"* [954]*.*

In order "*to determine whether someone has been 'deprived of his liberty'"*[955], the ECtHR appreciates the "*concrete situation*"[956] and takes into account "*a whole range of criteria such as the type, duration, effects and manner of implementation of the measure in question*"[957], knowing that "*a deprivation of liberty is not confined to the classic case of detention following arrest or conviction, but may take numerous other forms*"[958].

Furthermore, the ECtHR considers that "*the difference between restrictions on movement serious enough to fall within the ambit of a deprivation of liberty under Article 5§1 and mere restrictions of liberty which are subject only to* (the protection granted to the freedom of movement) *is one of degree or intensity, and not one of nature or substance*"[959].

The right to liberty and security "*is of the highest importance in a 'democratic society' within the meaning of the Convention*"[960], since personal liberty is considered to be *"a fundamental condition, which everyone should generally enjoy",* since *"its deprivation is something that is also likely to have a direct and adverse effect on the enjoyment of many of the other rights, ranging from the right to family and private life, through the right to freedom of assembly, association and expression to the right to freedom of movement*"[961]. Furthermore, "*any deprivation of liberty will invariably put the person affected into an extremely vulnerable position, exposing him or her to the risk of being subjected to torture and inhuman and degrading treatment*"[962].

---

[952] Monica Macovei, *The right to liberty and security of the person, A guide to the implementation of Article 5 of the European Convention on Human Rights*, Human rights handbooks, No. 5, Council of Europe, 2002, p. 8, http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-05(2004).pdf (last accessed on 31 May 2017).

[953] *Ibid.*, p. 8.

[954] *Ibid.*, p. 8.

[955] ECtHR, Guide on Article 5 of the Convention, Right to liberty and security, 2014, *op. cit*., p.5, §5.

[956] *Ibid*., p. 5, §5.

[957] *Ibid.*, p. 5, §5. The Court refers to the following decisions: Guzzardi v. Italy, § 92; Medvedyev and Others v. France [GC], § 73; Creangă v. Romania [GC], § 91).

[958] *Ibid.*, p. 5, §3. The Court refers to the following decision: *Guzzardi v. Italy*, § 95.

[959] *Ibid.*, p. 5, §2. The Court refers to the following decisions: *Guzzardi v. Italy*, § 93; *Rantsev v. Cyprus and Russia*, § 314; *Stanev v. Bulgaria* [GC], § 115.

[960] *Ibid.*, p. 7, §20. The Court refers to the following decisions: *Medvedyev and Others v. France* [GC], § 76; *Ladent v. Poland*, § 45, 18 March 2008.

[961] Monica Macovei, *The right to liberty and security of the person, A guide to the implementation of Article 5 of the European Convention on Human Rights*, *op. cit.* p. 7-8.

[962] *Ibid.*, p. 8.

4.8.3 Nature and extent of the right to liberty and security

The principle of the protection is that "*any deprivation of it should always be exceptional, objectively justified and of no longer duration than absolutely necessary*"[963].

More precisely, "*a person can only be deprived of* (...) (this freedom) *it in exceptional circumstances*"[964], the detention must be lawful[965] which has a very limited meaning[966] and imposes inter alia that the legal basis is clear, foreseeable, precise (satisfying the principle of legal certainty)[967] and provides for appropriate "*guarantees against the risk of arbitrariness*"[968], including in principle a court order and a reasoning in it[969]. In addition, a restriction of the freedom is not admitted for grounds other than one of the six ones *"exhaustively listed in Article 5 (1)"*[970].

4.9 The freedom to conduct a business

Understanding the freedom to conduct a business requires addressing the protecting legal instruments of this freedom, the notion of "freedom to conduct a business", and the nature and extent of its protection.

4.9.1 Legal instruments protecting the right to conduct a business

At the international level, this freedom is not specifically protected, but might be considered to be "*a modern supplement to worker's rights*"[971] which is protected by Article 23 of the United Nations Universal Declaration of Human Rights, Article 6 of the International Covenant on Economic, Social and Cultural Rights (right to work) and to a certain extent in Article 27 of the United Nations Convention on the Rights of Persons with Disabilities.

At the Council of Europe level, the ECtHR has recognised certain elements of this right, "*particularly those deriving from the freedom to enjoy the right to property (Article 1 of the Protocol No. 1 to the ECHR (the right to enjoy one's property)) and those related to the freedom of expression (Article 10 of the ECHR, freedom of 'commercial' expression)*"[972]. In addition, the Council of Europe's European Social Charter (ESC), "*guarantees the right to*

[963] *Ibid.*, p. 8.

[964] *Ibid.*, p. 8.

[965] *Ibid.*, pp. 9, 10.

[966] *Ibid.*, pp. 12-14; ECtHR, Guide on Article 5 of the Convention, Right to liberty and security, 2014, *op. cit.*, II pp.7-9.

[967] ECtHR, Guide on Article 5 of the Convention, Right to liberty and security, 2014, *op. cit.*, p.8.

[968] Monica Macovei, *The right to liberty and security of the person, A guide to the implementation of Article 5 of the European Convention on Human Rights*, *op. cit.* p. 14.

[969] ECtHR, Guide on Article 5 of the Convention, Right to liberty and security, 2014, *op. cit.*, p.10.

[970] Monica Macovei, *The right to liberty and security of the person, A guide to the implementation of Article 5 of the European Convention on Human Rights*, *op. cit.* p. 12.

[971] European Union Agency for Fundamental Rights, *Freedom to conduct a business: exploring the dimensions of a fundamental right*, 2015, p. 10, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf (last accessed on 31 May 2017).

[972] *Ibid.*, p. 10.

work (Article 1) and more explicitly the right to earn one's "living in an occupation freely entered upon" (Article 1 (2)). This provision could be used under certain circumstances related to the freedom to conduct a business, in particular in cases where there are disproportionate obstacles to setting up a business in order to make a profit"[973].

At the European level, the freedom to conduct a business it is explicitly protected by article 16 of the EU Charter of Fundamental rights (EUCFR) which states: "*The freedom to conduct a business in accordance with Community law and national laws and practices is recognised*".

4.9.2 The notion of freedom to conduct a business

According to the text of the explanations relating to the complete text of the Charter[974], the explicit consecration of this right is the result of "*Court of Justice case law which has recognised freedom to exercise an economic or commercial activity*"[975] and of Article 4 of the Treaty establishing the European Community recognising free competition.

In principle, this right refers to the right to conduct "*any legitimate form of profit-making activity conducted by one or several individuals 'in company'. The right seems to encompass the full 'life-cycle' of such activities, for instance from setting-up a company, through operating one, to insolvency or closing a business*"[976].

4.9.3 Nature and extent of the right to the freedom to conduct a business

According to the text of the explanations relating to the complete text of the Charter[977], "*this right is to be exercised with respect for Community law and national legislation. It may be subject to the limitations provided for in Article 52(1) of the Charter*".

Article 52 (1) of the EUCFR contains a principle inspired from the ECHR as regards the requirements for limiting conditional rights. These requirements, which apply to the freedom to conduct a business, are that "*any limitation (...) must be provided for by law and respect the essence of (the concerned) (...) rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".

---

[973] *Ibid.*, p. 10.

[974] European parliament, *Explanations relating to the Charter of Fundamental Rights of the European Union*, Art. 16 available from http://www.europarl.europa.eu/charter/convent49_en.htm and at ,http://www.europarl.europa.eu/charter/pdf/04473_en.pdf (URLs last accessed on 30 May 2017).

[975] Given references are the following : "*judgments of 14 May 1974, Case 4/73 Nold [1974] ECR 491, paragraph 14 of the grounds, and of 27 September 1979, Case 230-78 SPA Eridiana and others [1979] ECR 2749, paragraphs 20 and 31 of the grounds) and freedom of contract (see inter alia Sukkerfabriken Nykøbing judgment, Case 151/78 [1979] ECR 1, paragraph 19 of the grounds, and judgment of 5 October 1999, C-240/97 Spain v. Commission [not yet published], paragraph 99 of the grounds*".

[976] European Union Agency for Fundamental Rights, *Freedom to conduct a business: exploring the dimensions of a fundamental right*, 2015, *op. cit*. p. 11.

[977] European parliament, *Explanations relating to the Charter of Fundamental Rights of the European Union*, Art. 16 available from http://www.europarl.europa.eu/charter/convent49_en.htm and at ,http://www.europarl.europa.eu/charter/pdf/04473_en.pdf (URLs last accessed on 30 May 2017).

It must however be noted that the protection of this freedom, as well as in relation to the other rights protected by the ECFR only, "*applies only insofar as it relates to actions by EU institutions, or when Member States are acting within the scope of EU law*"[978]. As a consequence, if the basis for action is the EUCFR, "*the freedom to conduct a business is not applicable 'across the board'*", even though "*the CJEU has interpreted 'implementation by EU Member States' fairly broadly*"[979].

[978] European Union Agency for Fundamental Rights, *Freedom to conduct a business: exploring the dimensions of a fundamental right*, 2015, *op. cit*. p. 11.

[979] *Ibid.* p. 11.

5 Conclusion

Several fundamental rights and freedoms that might be impacted by the MANDOLA project have been studied in the current report. The protection they receive might differ depending on the legal basis that is used to enforce this protection, but the analysis shows that globally, Members States of the Council of Europe, which are also contracting parties to the European Convention on Human Rights and EU members, incorporate increasingly into their domestic law the jurisprudence of the European Court of Human Rights, thereby ensuring a certain harmonisation within the EU - and more globally within the Council of Europe area - of the protection of the fundamental rights and freedoms of citizens. The main remaining differences lie in the area of the fundamental rights and freedoms limitations that are authorised by the European Court of Human Rights, which are by definition not mandatory and fall therefore within the scope of the Member States' sovereign powers. This discussion will be continued in the MANDOLA deliverable D2.1, relating to the definition of illegal online hate speech.

6 List of main acronyms and abbreviations

CJEU: Court of Justice of the European Union.

DPIA: Data protection impact assessment.

ECHR: European Convention on Human Rights, referring to the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

ECtHR: European Court of Human Rights.

EU: European Union.

EUCFR: European Union Charter on Fundamental Rights.

GDPR or "General Data Protection Regulation": refers to Regulation (EU) 2016/679 of the European Parliament and of the Council 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[980].

ICTs: Information and communication technologies.

ISPs: Internet Service Providers.

LEAs: Law enforcement authorities.

PIA: Privacy impact assessment.

Police Directive or "Directive (on personal data protection) for the police and criminal justice sector": refers to the Directive (EU) 2016/680 of the European Parliament and of the Council on 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[981].

[980] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

[981] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

7 List of consulted experts

The following experts contributed to the current study by providing information relating to the legal framework of the country referred to before their name. They are the authors or main authors of the texts relating to this country, unless stated otherwise.

Belgium

- Mr. Bertrand Vandevelde, Attorney-at-Law, Demosdos.

Bulgaria

- Mrs. Ilona Krastenyakova, Prosecutor at the Supreme Prosecutor's Office of Cassation, Bulgaria (for ICITA).

Cyprus

- Mrs. Tatiana Synodinou, Associate Professor, Law Department University of Cyprus, Chair of the Ethics Committee of Mandola.

France

- Mrs. Estelle De Marco, Ph.D., senior researcher, Inthemis.

Germany

- Mr. Nicolas von zur Mühlen, Head of Section "Information Law and Legal Informatics", Max Planck Institute for Foreign and International Criminal Law.

Greece

- Mr. Ioannis Iglezakis, Associate Professor of Computers and Law, Faculty of Law of Thessaloniki, Faculty of Law, Aristotle University.

Ireland

- Mr. Hein Dries, LL.M, senior researcher, Aconite;
- Mrs. Estelle De Marco, Ph.D., senior researcher, Inthemis.

Netherlands

- Mr. Hein Dries, LL.M, senior researcher, Aconite;
- Mrs. Estelle De Marco, Ph.D., senior researcher, Inthemis.

Romania

- Mrs. Valentina Pavel Burloiu, independent researcher.

Spain

- Mrs. Miriam Guardiola, Attorney at Law.
- Mrs. Carmen Jorda, Attorney at Law and Researcher, UAM.