LaBoUR & Law Issues
Rights | Identity | Rules | Equality

GDPR and Personal Data Protection in the Employment Context

CLAUDIA OGRISEG
Università degli Studi di Milano

vol. 3, no. 2, 2017

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

GDPR and Personal Data Protection in the Employment Context

CLAUDIA OGRISEG
Università degli Studi di Milano
Dottoressa di ricerca in Diritto del Lavoro
c.ogriseg@studiomansi.com

ABSTRACT

Digital transformation and new technologies have completely overwhelmed the way to process personal data in the employment context.

This paper analyses how the right to protection of personal data has been codified in a multilevel legal framework (ECHR, EU Treaties, Directives and Regulations), how and if this right related to workers can prevail over the interests of companies, what guarantees are foreseen in the working context for the processing of personal data in Regulation 2016/679/EU (GDPR) and what kind of safeguards could be provided in each Member State.

In the GDPR, the right of employees to the protection of personal data is not particularly protected so as to prevail over the interests of companies. Despite the great importance of individual rights in the employment context, the European Union has failed to establish uniform rules. On this crucial issue we may have the opportunity to strengthen the protection of workers' rights, ensuring that personal autonomy is guaranteed and can be exercised by individuals even in the context of Big Data.

Keywords: GDPR; employee; employment; Big data; Big Data Management; HR Analytics; algorithms; personal data; employer; surveillance; electronic communications; new technologies; work; WP29; workplace; application and smart device; company property; labour relationship; legal ground; controller; data subject; Code of Civil Procedure; discrimination

GDPR and Personal Data Protection in the Employment Context

SUMMARY: 1. Introduction. - 2. From the Respect of Private and Family Life to the Right of Data Protection. - 3. The Right of Data Protection in the GDPR. - 4. Data Processing at Work in GDPR: the WP29 Opinion 2/2017. - 5. The Risks Analysis and Proportionality Assessment proposed in the WP29 Opinion 2/2017: Recruitment Process, In-employment Screening and Monitoring at the workplace and outside it. - 6. GDPR Member State Possibility to Ensure Workers' Right to Personal Data Protection. - 7. Conclusion.

1. Introduction

Digital transformation and new technologies have already completely overwhelmed our way to process personal data in the employment context.

It seems to be a disruptive innovation. The adoption of new forms of infrastructures, applications and smart devices enable employers to collect and connect each other with enormous quantities of employees' personal data and to do so within a reasonable time and with inexpensive means. New types of systematic and potentially pervasive data processing at work, less visible than traditional one such as overt CCTV cameras and more invasive of private life as employees work remotely, create significant challenges to privacy and data protection. This ongoing change is potentially huge and with far-reaching consequences. It involves the massive collection of employees' data (Big Data) and the algorithms use for predictive functions in the company's HR decision-making process (Big Data analytics or HR Analytics and Big Data Management) (1).

Despite the great importance of individual rights in the employment context, the European Union has not managed in stating a set of particular uniform rules for workers' data protection across the entire EU. Recital 4, General Data Protection Regulation 2016/679/EU (GDPR) states that the employees' right to the protection of personal data «must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality». Therefore, it will

(1) According to the European Union Agency for Network and Information Security, the term Big Data analytics «refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours» (ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015 https://www.enisa.europa.eu/publications/big-data-protection).

be crucial to carry out a new assessment of workers' right to the protection of personal data, especially since it is not considered as an "absolute right" in the new EU legal framework and each member States could provide more specific rules relating to this form of protection (Article 88 Regulation 2016/679/EU).

This paper analyses how the right to personal data protection has been codified in multilevel legal frameworks (CEDU; EU Treaties; Directives and Regulations), how and if this right could prevail over companies' interests, what kind of safeguards are provided for workers in GDPR and what kind of safeguards could be provided in each member States.

It is argued that personal data protection, first codified as a right to respect the private life and then as a freedom and an individual human right, is not preserved in GDPR for workers with special rules. Employees' right of data protection is not particularly safeguarded in such a way as to prevail over companies' interest to improve business through processing personal data. In the GDPR uniform framework it should be always a balance between employees' and companies' right and interests. This is clear in the documents issued by the Independent EU Advisory Body on Data Protection and Privacy (Article 29 Working Party so called "WP29") that anticipate the future work of the European Data Protection Board (EDPB) in issuing guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR (Article 70 par.1 (e), Regulation 2016/679/EU).

Anyway, if on one hand GDPR does not provide particular set of uniform rules to protect employees across the entire EU, on the other hand it allows each member State to issue special rules to safeguard the workers' right of personal data. On this crucial matter we could have different national rules, but also the opportunity to strengthen workers' personal data protection in each member State: ensuring procedural rules thanks to Article 88 Regulation 2016/679/ EU. By this I mean that employee's individual rights could be strengthened adopting specific rules in Code of Civil Procedure to prevent the "use" of personal data unlawfully processed before the Courts. Moreover, employee's individual rights could be strengthened adopting a "discrimination presumption" in case of using algorithms' mechanism in HR management without a Privacy Ethical and Social Impact Assessment.

2. From the Respect of Private and Family Life to the Right of Data Protection

The Universal Declaration of Human Rights laid down for the very first time in 1948 a right to protection the individual's private sphere against intrusion from others, especially from the State (Article 21). This certainly influenced the promotion of individual human rights in Europe since the protection of personal data was initially guaranteed just as a "*right to respect for private and family life"* (Article 8, ECHR) (2).

Only in 1981 did Member States of the Council of Europe recognize a «*right to privacy with regard to automatic processing of personal data relating to him ('data protection')*» as a fundamental freedom (3). The *Convention* 108 *for the protection of individuals with regard to the automatic processing of personal data* is the first, and unique, legally binding international instrument in which European States defined the previous nucleus of rules (4): a universal standard, to all data processing in the digital area that would have been the basis for EU law, Treaties and Regulations (Directives and Decisions). The Directive 95/46/EC adopted in 1995 was «designed to give substance to the principles of the right to privacy already contained in the Convention no.108 (of the Council of Europe), and to expand them», since «free movement of goods, capital,

(2) Pursuant to Article 8 (2) European Convention on Human Rights, "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society […] for the protection of the rights and freedoms of others".

(3) https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

(4) The Convention dealt with obtaining and processing of "quality" data (i.e. adequate, relevant, not excessive and accurate) for specified legitimate purposes without using for incompatible ends and storing for longer than necessary with "appropriate" security measures «*against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination*» (Article 5 Convention Council of Europe 108/1981). The Convention also statues that «*personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards*» (Article 6 Convention Council of Europe 108/1981). It also enshrined a nucleus of individual's right: any person should have been enable to know if its own personal data is stored and, if necessary, to have it corrected and allowed derogation from those provisions only if it is provided by the law and constitutes «*a necessary measure in a democratic society in the interests of: protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others*» (Article 9, Conv. Council of Europe n.108, 1981). Finally the Convention regulated trans-border data flows imposing restrictions where legislation does not provide equivalent protection. European Union Agency for Fundamental Rights - Council of Europe - Registry of the European Court of Human Rights, *Handbook on European data protection law*, 2014.

services and people within the internal market required the free flow of data, which could not be realized unless the Member States could rely on a uniform high level of data protection» (5).

Additionally, more detailed data protection EU provisions were issued (6), but the right of protection personal data has been definitively guaranteed as a "fundamental right of freedom" in the European Union only on 1st December 2009 with the coming into force of the Lisbon Treaty. As a matter of fact, the Article 6 par 1 of the Treaty of European Union (TUE) recognises "the rights, freedoms and principles" that were politically proclaimed nine years before with the Charter of Fundamental Rights of the European Union (hereinafter Charter) as adapted at Strasbourg and the contents of European Convention on Human Rights. Moreover, in Article 52 of the Charter, limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8, as long as these limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality (7).

(5) European Union Agency for Fundamental Rights- Council of Europe - Registry of the European Court of Human Rights, *Handbook on European data protection law*, 2014, p.17-18.

(6) The Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data; the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, (Data Retention Directive), invalidated on 8 April 2014.

(7) Article 52 - Scope and interpretation of rights and principles -1. Any limitation on the exercise of the rights and freedoms recognized by this Charter 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. 2.Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties. 3.In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection. 4.In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions. 5.The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union

The Title II of the Charter codifies the Right to liberty and security (Article 6), the Respect for private and family life (Article 7) and the Right to the protection of personal data (Article 8) (8). According to Article 8 of the Charter personal data «must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified» and «compliance with these rules shall be subject to control by an independent authority».

3. The Right of Data Protection in the GDPR

As contained in the EU legislation, European Parliament and the Council recognize Personal Data Protection as a fundamental freedom, repealing Directive 95/46/EC with the Regulation 2016/679/EU thanks to Article 16 par. 2 of the Treaty on the Functioning of the European Union (TFUE).

In this legal framework, the protection of physical person regarding processing of personal data involves a great effort to allow data processing on the basis of data subject's consent of the concerned or some other legitimate

law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality. 6. Full account shall be taken of national laws and practices as specified in this Charter. 7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States.

(8) Article 6 - 1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions. 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties. 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

basis and to design a strong set of rights to ensure each person a real «control of their own personal data» (9).

The European Union model of data protection recognises "data subject" a positive freedom to control and intervention (*recht auf Informationelle selbstbestimmung*) (10). The recognition of such wide control and intervention protection on personal data suggests Italian Authors to consider "data subjects" not as passive subjects suffering data processing but more as active entities leading to a definition of their own identity. Pursuant the Regulation 2016/679/EU the right of personal data protection is more safeguarded than in the Directive 95/46/EC. In Chapter II personal data shall be processed lawfully (if they fulfil specific applications such as data subject consent or another legitimate basis, laid down by law or the legitimate interests pursued by the controller), fairly in a transparent manner; data shall be collected for specified, explicit and legitimate purposes (Article 5-6-7). Moreover, controllers must do an analysis and risk assessment to define the appropriate measures (physical, logical and organizational) to assure integrity and security of data adequate, relevant and limited, accurate, kept with storage limitation (Article 5-6-7).

The "data minimisation" principle is particularly relevant in GDPR since digital transformation and data exchange have evolved making frequent data collection for a variety of treatments (11).

Regarding this set of rights, it is possible to point out that Regulation 2016/679/EU confirms with a great continuity Directive 95/46/EC, strengthening "data subjects' freedom": the right to live without arbitrary and unwarranted interference, intrusion or limitation. Considering the great technological evolution, the relevant perspective change in personal data protection is that the adequacy of measures adopted to protect the rights of a data subject must also be continuously tested and evaluated (the so called "risk based approach*"* Article 32 Regulation 2016/679/EU) (12).

(9) See recital 11 «Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States».

(10) Volkszählungsurteil (BVferG), 15 December 1983, 1 bVr 209/83.

(11) See CGCE, Google Spain SL, Google Inc. c. Agencia Española de Protectión de Datos, Mario Costeja Gonzales C-131/12 http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT .

(12) See WP29 Opinion 218/2014, *Statement on the role of a risk-based approach in data protection legal frameworks*.

In the next part of Regulation 2016/679/EU new tools are provided to guarantee each data subject which personal data can be processed to define "personal identity". In Chapter III data subjects' rights to receive transparent information, communication and modalities for the exercise of their rights (Article 12); information and access to personal data (Article 13-14-15 Regulation 2016/679/EU) are codified. These fundamental conditions protect "human identity" and let individuals decide which kind of personal data could be processed thanks to the recognition of the rights to rectification, erasure, restriction of processing, rights to data portability (Articles 16-17-18-19-20 Regulation 2016/679/EU).

The Regulation 2016/679/EU also imposes controllers to communicate the «breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed» to the individuals whose personal data have been affected by (Article 4 and Article 34). The Independent EU Advisory Body on Data Protection and Privacy outlines that new requirements strengthen data subjects' right since communicating a "data breach" to individuals allows them «to protect themselves from its potential consequences» (13).

As a matter of fact, with this last set of rights, GDPR upholds the previous protections recognizing greater force being placed on individual personal freedom. In the new legal framework, data subjects are able to control and define which personal data could be processed.

Moreover, the right not to be subject to an automated decision-making including profiling which produces legal effects is strengthened in Regulation 2016/679/EU (Articles 21-22). This was already provided in the Directive 95/46/EC (Article 15). But since the Council of Europe increasingly took into consideration this issue in Recommendation CM/Rec(2010)13, the lawfulness of automatic processing of personal data in the context of profiling depends on the adoption of particular and "adequate" safeguards. Following from Regulation 2016/679/EU data subjects are protected with the right to receive specific information on mathematical procedures; the right to obtain a human intervention in decision-making; the right to express opinion and receive an explanation on the decision and, above all, the right to contest and appeal against the decision (see recital 71 and Article 22). Regarding the Independent EU Advisory Body on Data Protection and Privacy «human intervention is a

(13) See WP29 *Guidelines on Personal data breach notification under Regulation 2016/679*, 3 October 2017.

key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject» (14).

The Authors stressed that Regulation 2016/679/EU grants a vital acknowledgement: «[i]t stands to reason that an algorithm can only be explained if the trained model can be articulated and understood by a human. It is reasonable to suppose that any adequate explanation would, at a minimum, provide an account of how input features relate to predictions» (15). On the other hand, it is said that the right of explanation is «a harmful-restriction for artificial intelligence» since «it is often not practical or even possible, to explain all decisions made by algorithms» (16). The "big question" remains how this language affects deep neural networks that depend on vast amounts of data and generate complex algorithms that can be opaque even to those who put these systems in place (17). Predictive strategies based on algorithms could at the same time lead to systematic injury to human dignity and to the principle of non-discrimination, guaranteed to freedom of thought, choice and action (18).

4. Data Processing at Work in GDPR: the WP29 Opinion 2/2017

The new perspective change in GDPR personal data protection is clearly evident in the Opinion 249/2017 *on the processing of personal data in the employment context* issued by the Independent EU Advisory Body on Data Protection and Privacy (Article 29 Working Party so called WP29).

It must be evidenced that in GDPR the employee is not reserved for a particular set of protections against any one "data subject". Despite the great

(14) See WP29 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 3 October 2017.

(15) B. Goodman B. - S. Flaxman, *European Union regulation on algorythmic decision-making and a "right to explanation"* https://arxiv.org/pdf/1606.08813.pdf

(16) N. Wallace, *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence* January 2017 http://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm

(17) V. Mayer-Schönberger, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation* http://www.stlr.org/cite.cgi?volume=17&article=SchonbergerPadova

(18) Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016 https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

importance of individual rights at the workplace evidenced by the WP29 in the last decade (19), the European Union has not managed even this time in regulating the employment context with uniform specific binding EU rules (20).

Regarding data processing at work in the Regulation 2017/679/EU Article 9 merely provides for an exemption from the prohibition on processing sensitive data in the labor field and Article 88 is limited to allow member State to define specific rules to protect employees' right to personal data. From this viewpoint is important to analyze how the WP29 outlines the employees' risks to personal rights posed by new technologies and undertakes a general proportionality assessment, balancing the employees' rights and the employers' legitimate expectation to process personal data in managing human resources.

Referring to all workers (21), in the Opinion 2/2017 it is stressed that consent cannot legitimate data processing in the employment context due to the nature of the labor relationship (22). As a matter of fact, pursuant to the new rules on consent in GDPR, employees' consensus could hardly legitimate the personal data process, since the typical dependency of the labor relationship that rarely puts workers in a position to freely give, refuse or revoke consent.

(19) See http://ec.europa.eu/newsroom/article29/news-overview.cfm and in particular the Opinion 8/2001 *on the processing of personal data in the employment context* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp48_en.pdf and the 2002 Working Document *on the surveillance of electronic communications in the workplace* 29 May 2002, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2002/wp55_en.pdf .

(20) The interest of the matter is evident but in the Directive 95/46/CE, Article 27 merely promoted the development of codes of conduct in labor contract as a particular area: «*The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors*». Other documents on this matter were not binding: (Communication (97) 290, *The social and labour market Dimension of the Information Society; People First-Next Steps*; Communication from the Commission, *First stage consultation of social partners on the protection of workers' personal data*, 2001; Communication from the Commission, Second stage consultation of social partners on the protection of workers' personal data, 2004) and a Recommendation of the Council of Europe (2015) 5.

(21) The term "*employee*" «*is intended to cover all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract*».

(22) «*Employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. (So) Unless in exceptional situations, employers will have to rely on another legal ground than consent – such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees*».

As previously outlined also in Opinion 8/2001, the legal basis for such data processing could normally be "performance of a contract" (meeting obligations under labor contract such as paying a salary, requiring the processing of personal data - Article 7 (b) Regulation 2016/679/EU; "legal obligations" imposed on the employer by employment law (where law constitutes the legal basis for the data processing) (Article 7 (c) Regulation 2016/679/EU) or the employer "legitimate interest" (Article 7 (f) Regulation 2016/679/EU). This final legal basis for processing implies specific mitigation measures to ensure a proper balance between the employer legitimate interest and employees' fundamental rights and freedoms: monitoring limitation (geographical; data oriented; time-related) and appropriate technical and organizational measures.

In the Opinion 2/2017 it is outlined that in most cases, the legitimate interest of companies could be invoked to process employees' data. This will imply a proportionality test (whether data are necessary, whether the processing outweighs the data protection rights) and an evaluation about what kind of measures should be taken to ensure the right to a private life and the right to secrecy of communications. In other words, for WP29 the processing purpose must be legitimate and the chosen method proportional to the business needs: «Data processing at work should be carried out in the least intrusive manner possible and be targeted to the specific area of risk».

Moreover, regardless of the legal basis, all processing operations must comply with the principle of transparency (Article 10 and 11 Regulation 2016/679/EU). Employees must always be clearly and fully informed with effective communication. The WP29 «recommends involving a representative sample of employees in the creation and evaluation of such rules and policies». The new requirements introduced by GDPR imply, for data controllers, to implement security measures (appropriate technical and organizational measures: see Article 17 Regulation 2016/679/EU). Moreover the new requirements grant employees the right not to be subject to an automated decision (Article 15 Regulation 2016/679/EU) and prevent the most privacy-friendly solutions with data minimization (data protection "by design and by default").

Last but not least, according to GDPR the employer should carry out a Data Protection Impact Assessment (DPIA) if «a type of processing, in particular using new technologies, and taking into account the nature, scope and context and purpose of the processing itself is likely to result in a high risk to the rights and freedoms of natural persons» (Article 35 Regulation

2016/679/EU). Regarding recitals 71 and 91 Regulation 2016/679/EU "result in a high risk" evaluation or scoring, including profiling and predicting, especially from «aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements». The WP29 outlines that a DPIA is likely to be required if «a company systematically monitor(s) its employees' activities, including the monitoring of the employees' work station, internet activity» since it implies a «systematic monitoring and data concerning vulnerable data subjects» (23).

The DPIA should evolve in a Privacy Ethical and Social Impact Assessment (PESIA) (Mantelero 2016). «According to the need to balance all interests concerned in the processing of personal data, and in particular where information is used for predictive purposes in decision-making processes, controllers and processors should adequately take into account the likely impact of the intended Big Data processing and its broader ethical and social implications to safeguard human right and fundamental freedoms, and ensure the respect for compliance with data protection obligations as set forth by Convention 108» (24).

5. The Risks Analysis and Proportionality Assessment proposed in the WP29 Opinion 2/2017: Recruitment Process, in employment Screening and Monitoring at the workplace and outside it

According to the new perspective changing in the GDPR legal framework WP29 proposes a risk analysis on employees' data protection and a proportionality assessment. In Opinion 2/2017 the Independent EU Advisory Body analyses some scenarios in which data processing in the employment context could have the potential to damage employees' rights and stresses the

(23) See WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, last revised and adopted on 4 October 2017.

(24) See the *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* of the Council of Europe. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasburg 23 January 2017 in https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a.

importance of finding a possible balance between workers' data protection right and companies' interests.

Regarding WP29, the first personal data processing potentially damaging for workers deals with recruitment. It referees to the «use of social media by individuals is widespread and it is relatively common for user profiles to be publicly viewable depending on the settings chosen by the account holder». In Opinion 2/2017 such a data process is considered lawful thanks to the legal grounds of "legitimate interest" (Article 7 (f) Regulation 2016/679/EU: the employer is «allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for» but the candidates must be correctly informed (for example in the job advert).

The risk analysis and assessment proposed is important. It points out that "individual consent" during recruitment or in the employment context could not be a lawful legal ground for data processing, given the unequal relationship between the employee and the employer. In Opinion 2/2017 it is said that in the employment context the personal data process should be legitimate by legal grounds different from consent and in any case, should be proportionate, subsidiary, minimized and informed. Regarding WP29 the information on data process should communicate to workers whether companies process data publicly-available on various social networks.

In the Opinion 2/2017 it is stressed that «employers have (or can obtain) the technical capability of permanently screening employees by collecting information regarding their friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviors therefore capturing data, including sensitive data, relating to the employee's private and family life». But it is also outlined that «in-employment screening of employees' social media profiles should not take place on a generalized basis» and «moreover, employers should refrain from requiring an employee or a job applicant access to information that he or she shares with others through social networking». It is said that monitoring or screening individuals (candidates or workers) should be related to business or private purposes, necessary «to protect (company's) legitimate interests» proportionate in the absence of «other, less invasive means available», transparent since «the former employees (should be) adequately informed about the extent of the regular observation of their public communications» and, above all, should respect the employee's private and family life rights.

This point is critical and it deals with the respect of private life and family life and with the lawfulness of limiting ancillary obligations in labor agreements. Using a social media profile could be contractually provided in the light of employee's tasks. Moreover, a worker's personal identity shown in an official profile on social networks could affect corporate image so it would always be better if clearly specified in the terms and conditions to set out clearly it in the employment contract. The fair balance, between workers' data protection right and companies' interests, suggested in the Opinion 2/2017 recommends to protect workers right to «retain the option of a "non-work" non-public profile that they can use instead of the "official" employer-related profile, and this should be specified».

The other scenario in which processing employees' personal data could be potentially damaging is concerned with the control on electronic communications in the workplace (e.g., phone, internet browsing, email, instant messaging, VOIP, etc.).

The conclusion in relation to the e-mail monitoring and use of internet remain valid, as referred to in 2001 Working Document on the surveillance of electronic communications in the workplace. Thus, «it is possible that an employer will implement an "all-in-one" monitoring solution, such as a suite of security packages which enable them to monitor all ICT usage in the workplace as opposed to just email and/or website monitoring as was once the case».

In the Opinion 2/2017 it is outlined that «the legal basis of Article 7(f) is only available if the processing meets certain conditions. Firstly, employers utilizing these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology. Secondly, employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organization's network and equipment, and strictly detailing the processing taking place». Thirdly, the requirement of subsidiarity implies to give "prevention much more weight than detection". For example, if there is a prohibited use of communications, «block(ing) websites instead of continuously monitoring all communications should be chosen in order to comply with this requirement of subsidiarity».

The other scenario, considered in the Opinion 2/2017, is data processing operations resulting from monitoring ICT usage outside the work

place. This practice is becoming more common since the growing of home and remote working. In Italy the possibility to recognize employee to work everywhere outside the company has been recently codified in law (the so - called *smart work*: Act no.81/2017). Such labor relation «involves the employer issuing ICT equipment or software to the employees which, once installed in their home/on their own devices, enables them to have the same level of access to the employer's network, systems and resources that they would have if they were in the workplace, depending on the implementation». In the Opinion 2/2017 it is outlined that remote working presents additional risks for companies' data security «without the implementation of appropriate technical measures the risk of unauthorized access increases and may result in the loss or destruction of information, including personal data of employees or customers, which the employer may hold».

The requirement to mitigate the risks for data protection could suggest employers being allowed in «deploying software packages (either on-premise or in the cloud) that have the capabilities of, for example, logging keystrokes and mouse movements, screen capturing (either randomly or at set intervals), logging of applications used (and how long they were used for), and, upon compatible devices, enabling webcams and collecting the footage thereof». Contrary to this, in the Opinion 2/2017 it is stressed that «the processing involved in such technologies are disproportionate and the employer is very unlikely to have a legal ground under legitimate interest, e.g. for recording an employee's keystrokes and mouse movements». The fair balance suggested in the Opinion 2/2017 implies «addressing the risk posed by home and remote working in a proportionate, non-excessive manner» in other words the company must comply with Deming Cycle, defining proportionate data protection measures by default and by design.

What is certain is that risks on employees' rights could increase since the rising popularity of electronic devices and the recent widespread practice to "Bring Your Own Device" [BYOD] at work: «employees' use of their own devices will lead to employers processing non-corporate information about those employees, and possibly any family members who also use the devices in question». In the Opinion 2/2017 it is stressed that «monitoring the location and traffic of such devices may be considered to serve a legitimate interest to protect the personal data that the employer is responsible for as the data controller; however this may be unlawful where an employee's personal device is concerned, if such monitoring also captures data relating to the employee's private and family life». The fair balance proposed in the Opinion 2/2017

suggests to «distinguish between private and business use of the device appropriate measures», «implement methods by which their own data on the device is securely transferred between that device and their network (i. e. configuring device to route all traffic through a VPN back into the corporate network, so as to offer a certain level of security)»; use devices «that offer additional protections such as "sandboxing" data (keeping data contained within a specific app)» or at least prohibit «the use of specific work devices for private use if there is no way to prevent private use being monitored».

Continuous monitoring should be possible also thanks to Mobile Ddevices Management (MDM). Such tools let the employer locate devices remotely, deploy specific configurations and applications and delete data on demand. In the Opinion 2/2017 it is suggested to perform a Data Privacy Impact Assessment (DPIA) and to value whether the resulting «data processing complies with the principles of proportionality and subsidiarity». Data collection should respect a specific purpose, «could not form a part of a wider program enabling ongoing monitoring of employees" and "tracking features should be mitigated» to become «available only in circumstances where the device would be reported or lost».

Wearable devices could enable the employer to process personal data which is potentially really damaging for employees since they collect health data and activity, sometimes even outside the workplace. The sensitive nature of data involves an unlawful data process and is prohibited for employer (Article 8 Regulation 2016/679/EU). As it is described in Opinion 5/2014 on Anonymisation Techniques, it is technically very difficult to ensure complete anonymisation of the data.

The 'badge' and systems that enable employers to control entrances and exits from certain areas could be potentially damaging for employees, since new technologies can allow tracking «employees' time and attendance are being more widely deployed, including those that process of biometric data as well as others such as mobile device tracking»". In Opinion 2/2017, the processing could be necessary and lawful in the legitimate interests of the employer under Article 7(f) and should not overweight employees' right to data protection if the system is installed in order to comply with legal obligations to secure the data against unauthorized access. «However, the continuous monitoring of the frequency and exact entrance and exit times of the employees cannot be justified if these data are also used for another purpose, such as employee performance evaluation».

Similarly disproportionate to the rights and freedoms of employees, and, therefore, generally unlawful, could be monitoring and surveillance by video or by technologies installed on company vehicles. The application of technology on video could allow employer «to access the collected data remotely (e.g. via a smartphone) easily (with a) (…) reduction in the cameras' sizes (along with an increase in their capabilities, e.g. high-definition)» and to process data performing by new video analytics (for example monitoring facial expressions by automated means, identifying deviations from predefined movement patterns and more). In Opinion 2/2017, it is stressed that the processing could also involve profiling and automated decision-making and that a fair balance «should refrain employers from the use of facial recognition technologies».

Telematics vehicles could allow employer to collect *data* about both the vehicle and the driver: not just the location of the vehicle (and, hence, the employee) by basic GPS tracking systems, but also a wealth of other information including driving behavior or even an event. «Employers might be obliged to install tracking technology in vehicles to demonstrate compliance with other legal obligations, e.g. to ensure the safety of employees who drive those vehicles» or he could «have a legitimate interest in being able to locate the vehicles at any time». A legal basis for monitoring employees and the vehicles' locations can easily be found, however, in a fair balance in the Opinion 249/2017 is outlined that «it should first be assessed whether the processing for these purposes is necessary, and whether the actual implementation complies with the principles of proportionality and subsidiarity. (…) For example, this could mean that, in order to prevent car theft, the location of the car is not registered outside working hours, unless the vehicle leaves a widely defined circle (region or even country). In addition, the location would only be shown in a "break-the-glass" way - the employer would only activate the "visibility" of the location, accessing the data already stored by the system, when the vehicle leaves a predefined region».

As stated in the WP29 Opinion 13/2011 on Geolocation services on smart mobile devices «the employer must clearly inform the employees that a tracking device has been installed in a company vehicle that they are driving, and that their movements are being recorded whilst they are using that vehicle (and that, depending on the technology involved, their driving behaviour may also be recorded). Preferably such information should be displayed prominently in every car, within eyesight of the driver». In particular, if the use of a private vehicle is allowed, the most important measure «an employer can

take to ensure compliance with (…) (GDPR) principles is the offering of an opt-out: the employee in principle should have the option to temporarily turn off location tracking when special circumstances justify this turning off, such as a visit to a doctor».

The European Court of Human Rights likewise confirmed the lawful of GPS surveillance and the processing and use of the data of a suspected of involvement in bomb attacks by a left-wing extremist movement since the monitoring «had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime (and) it had also been proportionate: GPS surveillance had been ordered only after less intrusive methods of investigation had proved insufficient, had been carried out for a relatively short period (some three months), and had affected the applicant only when he was travelling in his accomplice's car» (25).

Similarly, there are event data recorders being placed into vehicles that could enable the employer to record at certain times, abrupt directional change or accidents, but could also be set to monitor continuously, to observe and review an individual's driving behaviour with the aim of improving it. In the Opinion 2/2017 «the continuous monitoring of employees with such cameras constitutes a serious interference with their right of privacy». Opting for a fair balance, it is suggested to use «other methods (e.g., the installation of equipment that prevents the use of mobile phones) as well as other safety systems like an advanced emergency braking system or a lane departure warning system that can be used for the prevention of vehicle accidents which may be more appropriate».

For all of the applications mentioned above that could allow a form of continuous employees' monitoring and surveillance «the employer must ensure that the collected data are not used for illegitimate further processing, such as the tracking and evaluation of employees». The WP29 seems to have adopted a stricter interpretation of the employee's rights respect CEDU (26). In a recent pronunciation the Court statues that the notification about the possibility of monitoring correspondence and other communications should be clear about the nature of the monitoring and be given to employee in advance; that the monitoring should be limited in time and in the number of people who had access to the results; that the monitoring requires weightier justification since is more invasive method; that the monitoring system should

(25) CEDU, 2 September 2010, Uzun v. Germany (application no. 35623/05) https://hudoc.echr.coe.int/eng-press#{"itemid":["003-3241790-3612154"]}

(26) See http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

be based on less intrusive methods and measures than directly accessing the content of the employee's communications (27).

Last but not least, other two scenarios involved in the Opinion 2/2017 refer both to the employees' *data* disclosure to third parties and to international transfer of HR *data*.

Regarding employee's data disclosure to customers in the Opinion 249/2017 it is clear that providing third parties with employees' passport photos or location could have a legal standing only if in the employer's legitimate interest (Article 7 (f) Regulation 2016/679/EU), since employees would not be in a position to give free consent. However, such data processing should be proportionate to have a legal standing.

As regards HR trans-border data flow, as previously outlined in Opinion 8/2001, the transferring of personal data to a third country outside the EU (which is not a synonym of communication) (28), could take place only if an "*adequate level of protection*" is ensured. As previous Art. 25 Directive states, the *adequate level* must be related with an effective protection of individual rights. «It should thus be ensured that these provisions concerning the international transfer of data are complied with. WP29 re-states its previous position that it is preferable to rely on adequate protection rather than the derogations listed in Art. 26 of the DPD; where consent is relied on it must be specific, unambiguous and freely-given. However, it should also be ensured that the data shared outside the EU/EEA, and subsequent access by other entities within the group, remains limited to the minimum necessary for the intended purposes».

6. GDPR Member State Possibility to Ensure Workers' Right to Personal Data Protection

Each member State has the chance to strengthen the workers' personal data protection: providing for procedural rules. Article 88 par. 1 Regulation 2016/679/EU codifies the purposes of these specific rules: recruitment; performance of the employment contract (including discharge of obligations laid down by law or collective agreements); management, planning and organization of work; equality and diversity in the workplace; health and safety

(27) CEDU Grand Chamber 5 September 2017, *Bărbulescu v. Romania* (application no. 61496/08 http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

(28) CGCE 6 November 2003, Bodil Lindqvist C-101/01.

at work; protection of an employer's or customer's property; exercise and enjoyment (on an individual basis) of rights and benefits related to employment; termination of the employment relationship. Moreover, such rules should include particular measures to safeguard employees' human dignity, legitimate interests and fundamental rights, with particular regard to: the transparency of processing; the transfer of personal data within a group of undertakings or group of enterprises engaged in a joint economic activity; and monitoring systems at the workplace (Article 88 par. 2 Regulation 2016/679/EU).

In Italy, Article 13 Act 25 October 2017, no.163 published in the G.U. no.259 on the 6th November 2017 gives the Government the power to adopt GDPR into national legislation (29). It provides the Government with a few tasks: repealing the part of Italian Code of Privacy which is in contrast with GDPR; changing the Italian Code of Privacy to implement GDPR; coordinating the Italian Code of Privacy to GDPR; implementing specific measures adopted by the Italian Independent Body of Data Protection; adapting the Italian sanctions system to GDPR.

The delegation mentioned above is synthetic but general, and it could allow the Government to strengthen workers' personal data protection.

Regardless the importance of recognizing any real effectiveness to employees' data protection rights, it could be crucial first of all to issue rules in the Code of Civil Procedure, in the case of unlawful data processes. This kind of measure involves also specific rules of Civil Procedure about digital evidence classified as «data (comprising the out put of analogue evidence devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication» (30). We should take into account that **«**the very nature of data and information held in electronic form makes it easier to manipulate than traditional forms of data, that all legal proceedings rely on the production of evidence in order to take place and that electronic evidence is no different from traditional evidence in that is necessary for the party introducing it into

(29) http://documenti.camera.it/Leg17/Dossier/Pdf/ID0029B.Pdf.

(30) S. Mason, *Electronic Evidence: Disclosure, Discovery and Admissibility*, London, LexisNexis Butterwords, 2007.

legal proceedings, to be able to demonstrate that it is no more and no less than it was, when it came into their possession» (31).

Moreover, it could be opportune to give effectiveness to employee's right of data protection ensuring a "privileged access" to anti-discriminatory remedies inverting the onus of proof in case of using algorithms' mechanism in HR management without a Privacy Ethical and Social Impact Assessment (PESIA).

7. Conclusion

The right to *personal data protection* has been codified in multilevel legal frameworks (CEDU; EU Treaties; Directives and Regulations), first as a right to respect private life and then as a freedom and an individual human right. At the moment, pursuant to GDPR, this individual right allows an employee to control each their own data process or each their own personal identity. A personal identity that is a result of a diachronic identification process of each human being (32). Outlining our personal identities, we tread a path dotted by choices, not always explicit and conscious but negotiated and revisable (33). Multiple parts of information or factors that could be the makings of personal identity often co-exist during the life.

Each one of us should have the freedom to decide which ~~one~~ identity should prevail in the context of employment. Freedom allows us that kind of choice regarding standards belonging to social collective microcosms (34). The right to protect personal data recognises a control on the "personal hologram" accuracy cyclically defined through our personal data collected and correlated by others.

However, this individual right is not absolute and it does not always prevail over companies' interests to improve business through processing personal data. The analysis and risk assessment on the employees' right to

(31) SADFE2015, *Proceedings of the 10th International Conference on Systematic Approaches to Digital Forensic Engineering* in http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/SADFE-2015-Proceedings.pdf.

(32) R. Posner, *Are We One Self or Multiple Selves? Implications for Law and Public Policy*, in *Legal Theory*, 1997, 3, 23-35.

(33) G. Pino, *L'identità personale* in S. Rodotà – M. Tallacchini (a cura di), *Ambito e fonti del biodiritto*, in S. Rodotà – P. Zatti (diretto da), *Trattato di biodiritto*, Milano, Giuffré, 2010.

(34) K.A. Appiah, *The Ethics of Identity*, Princeton, NJ, Princeton University Press, 2005.

protect personal data proposed in the Opinion 2/2017 on the processing of personal data in the employment context suggests that workers are in a weak position. This could be true especially as regards the Human Resource Analytics (HR Analytics) that refer to applying analytic processes to the human resource department of an organization in the hope of improving employee performance and, therefore, getting a better return on investment.

Naturally the Big Data Challenge is promoting fairness, ethics, and mechanisms for mitigating discrimination in employment opportunity. The DPIA should evolve in a Privacy Ethical and Social Impact Assessment (PESIA) (35), but it might not be enough. It might be reasonable to prevent companies from acquiring an excessive power on processing Big Data and to enforce the rights of control and autonomous choice of personal data in a form of self-determination for individuals.

Moreover, it could be crucial «to ensure that personal autonomy and the right to control personal data are guaranteed and can be exercised by individuals in a Big Data context» (36). Workers' rights in each member State should be strengthened by providing civil procedural rules ~~tools~~ to carry this out, thanks to Article 88 Regulation 2016/679/UE.

(35) A. Mantelero, *Personal data for decisional purpose in the age of analytics: From an individual to a collective dimension of data protection* in *Computer Law and Security Review*, 2016, 32, 245.

(36) Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasburg 23 January 2017 in https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a.

Bibliography

Appiah K.A., *The Ethics of Identity*, Princeton, NJ, Princeton University Press, 2005.

Bevitt A. – Stack C., *Preparing for the GDPR – advice for employers*, Privacy&Data Protection Journal (PDP), https://www.cooley.com/files/Preparing%20%for%20the%20GDPR.pdf

ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015 https://www.enisa.europa.eu/publications/big-data-protection

Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016 https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

Goodman B. – Flaxman S., *European Union regulation on algorythmic decision-making and a "right to explanation"* https://arxiv.org/pdf/1606.08813.pdf

Goodman B., *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection* http://www.mlandthelaw.org/papers/goodman1.pdf

Mayer-Schönberger V., *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation* http://www.stlr.org/cite.cgi?volume=17&article=SchonbergerPadova.

Mantelero A., *Personal data for decisional purpose in the age of analytics: From an individual to a collective dimension of data protection* in *Computer Law and Security Review*, 2016, 32, 245.

Mason S., *Electronic Evidence: Disclosure, Discovery and Admissibility*, London, LexisNexis Butterwords, 2007.

Pino G., *L'identità personale* in S. Rodotà – M. Tallacchini (a cura di), *Ambito e fonti del biodiritto*, in S. Rodotà – P. Zatti (diretto da), *Trattato di biodiritto*, Milano, Giuffré, 2010

Pizzetti F., *Intelligenza artificiale e salute: il sogno dell'immortalità alla prova del GDPR* 15 settembre 2017 https://www.agendadigitale.eu/sicurezza/intelligenza-artificiale-e-salute-il-sogno-dellimmortalita-alla-prova-del-gdpr/

Posner R., *Are We One Self or Multiple Selves? Implications for Law and Public Policy*, in *Legal Theory*, 1997, 3, 23-35.

SADFE 2015, *Proceedings of the 10th International Conference on Systematic Approaches to Digital Forensic Engineering* in http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/SADFE-2015-Proceedings.pdf

Sen A., *Identity and Violence*, London, Allen Lane, 2006

Wallace N., *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence* January 2017 http://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm

Allegati:

Link text *Opinion paper 249/2017 on data processing at work* of Article 29 Data Protection Working Party, 8 June 201: https://t.co/FNH77m3b5B.