European Journal of Privacy Law & Technologies



2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

EDITOR IN CHIEF/DIRECTOR
Prof. Avv. Lucilla Gatt – Università Suor Orsola Benincasa di Napoli

VICE DIRECTOR
Prof. Ilaria A. Caggiano - Università Suor Orsola Benincasa di Napoli

BOARD OF DIRECTORS – SCIENTIFIC COMMITTEE
Prof. Juan Pablo Murga Fernandez – Universidad de Sevilla
Prof. Alex Nunn – University of Derby
Prof. Roberto Montanari - Università Suor Orsola Benincasa di Napoli
Prof. Andrew Morris – University of Loughborough

REFEREES
Prof. Manuel Espejo de Torralba - Universidad de Sevilla
Prof. Maria A. Scagliusi – Universidad de Sevilla
Prof. Martin Maguire - University of Loughborough
Prof. Scott Atkins - University of Derby
Prof. Leslie Masters - Unversity of Derby

EDITORIAL TEAM
Coordinator:
Ph.D. Avv. Maria Cristina Gaeta - Università Suor Orsola Benincasa di Napoli

Members:
Prof. Hackeem Yusef - University of Derby
Prof. Manuel Pereiro Càrceles - University of Valencia
Prof. Sara Lorenzo Cabrera - Universidad de La Laguna
Avv. Delia Boscia - Ordine Avvocati Napoli
Ph.D. Avv. Anita Mollo - Università Suor Orsola Benincasa di Napoli
Avv. Flora Nurcato - Università Suor Orsola Benincasa di Napoli
Ph.D (c) Noel Armas Castilla - Universidad de Sevilla
Ph.D. Sara Saleri - Re:Lab
Ms. Aura Tardia - Re:Lab
Dr. Lucio San Marco - Giappichelli Editore

SUMMARY

pag.

Section I: Articles

VALERIA FALCE, *State aids between public fair and unfair competition* 1

MARIA ROBERTA PERUGINI AND DEBORAH CAPUTO, *Il Data Protection Officer: le caratteristiche e i connessi profili di responsabilità* 11

VALERIA MANZO, *The General Data Protection Regulation (GDPR) nella Pubblica Amministrazione* 30

EMILIANO TROISI, *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intellegibilità' dell'algoritmo* 41

VERONICA CARRIERO, *Smart contracts in the blockchain context: what happens?* 61

Section II: Comments on decisions

MARINÍ GAIA CHIACCHIO, Il trattamento illecito di dati personali in ambito processuale (commento a Cass. pen., sez. III, 29.5.2019, n. 23808) 65

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Octava), 12 diciembre 2013, *X*, C-486/12 74

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera), 7 noviembre 2013, *IPI*, C-473/12 76

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta), 17 octubre 2013, Michael Schwarz/Stadt Bochum, C-291/12 79

pag.

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera), 22 noviembre 2012, Probst, C-119/12 81

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), 16 octubre 2012, Comisión Europea/Austria, C-614/10 83

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), 9 marzo 2010, *Comisión Europea/Alemania*, C-518/07 85

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal Supremo (Sala 3a de lo Contencioso Administrativo), 3 octubre 2014, no. 3896 87

MARÍA BOCIO JARAMILLO, análisis de la Sentencia del Tribunal Supremo (Sala de lo Social), 13 mayo 2014, no. 2618 91

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal Supremo (Sala de lo Contencioso Administrativo), 10 noviembre 2011, no. 7583 94

ADRIÁN PALMA ORTIGOSA, análisis de la Sentencia del Tribunal Supremo (Sala de lo Contencioso Administrativo), 15 diciembre 2004 97

MARÍA BOCIO JARAMILLO, análisis de la Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo), 28 septiembree 2001, no. 5463 99

Section III: Use Cases

DAVIDE BORELLI, LUCILLA GATT, *Privacy by Design and by Default and Data Protection Impact Assessment (DPIA)* 101

VITTORIA RUSSO, MARIA CRISTINA GAETA, *Data Management* 105

ALEX NUNN, TAMSIN BOWERS-BROWN, *Data Security and Mobilising the Whole School Workforce to close Educational Attainment Gaps* 116

ANDREW MORRIS, MARTIN MAGUIRE, NATHAN STUTTARD, *Responding to a Data Breach in a Bank* 120

pag.

ANDREW MORRIS, MARTIN MAGUIRE, NATHAN STUTTARD, *Protecting data from theft* 124

AURA TARDIA, *Ensuring Data Protection in the Internet of Things Domain* 128

ROBERTO MONTANARI, ELISA LANDINI AND AURA TARDIA, *Embedding Privacy in New Technologies* 132

List of Authors 151

Section I: Articles

STATE AIDS BETWEEN PUBLIC FAIR AND UNFAIR COMPETITION

Valeria Falce

Summary: 1. The infringement of public rules and unfair competition. – 2. Unfair competition and tort law. – 3. State aids provisions and unfair competition. – 4. Evolution of the case law. – 5. Conclusions.

1. The infringement of public rules and unfair competition

The ongoing "administrativization" process of the legal system and of the market relations, together with the growing of legislative intervention (both European and national) designed to, in several respects, safeguarding the competition and protecting the market have renewed the debate on the cooperation on the enforcement of the relevant regulation.

In this context, the strengthened constitutional significance of the competition, combined with the importance of the codified provisions, in particular on unfair competition, suggest we should return to reflect on the assumptions in which the violation of a public provision in general, and specifically the violation of the provisions dedicated on State aids, constitutes a conduct affecting the professional correctness paradigm in contrast with the repressive rules on unfair competition pursuant to Article 2598 and following of the Italian Civil Code.

In order to provide a correct framework of the debate it should be approached from a dual perspective: firstly, a conduct may violate at the same time different legal assets, thus being subjected to as many grounds of censorship; secondly, a conduct may violate a legal asset that is protected in several ways by the legal system, in which case the operator, in identifying the applicable rules, is led by the criterion of the precedence of the special provision over the general provision, which withdraws.

Once the general principles are pointed out, the challenge is now to apply them to the particular case, in order to verify: i) if and to which extent the viola-

tion of a provision of public law, including the one which provides State aids, constitutes, at the same time, an act of unfair competition pursuant to Article 2598 of the Italian Civil Code; ii) if and to what extent the conformity of a conduct with a provision of public law, and furthermore with the provision on State aids, may represent an act of unfair competition.

In the first case *i)*, and as a first approximation, the issue must be resolved by using the theories on the cumulation of the disciplines and liabilities, in which respect there are three different interpretative lines: the first one, invoking the ethical concept of professional correctness, identifies an act of unfair competition in every violation of the public requirements by an entrepreneur [1]; the second one, by applying the corporate concept of fairness, rejects the cumulation of liabilities on the presumption of the takeover on the competitive impact of the conduct contrary to a public provision by the administrative or criminal impact of the same conduct which has been already punished under another title; the third one, enhancing the regulatory concept of professional correctness, is placed in an intermediate position since it states that the conduct contrary to a public provision may constitute a type of unfair competition or not, depending on the impact that the public provision and its violation will have on the proper functioning of the market and of the competition.

Unlike the first two lines of interpretation, the third one is prevailing because of its flexibility and inherent capacity to capture the complexity and structure of each individual case in such a way as to permit a suitable balancing. Following this strand, the challenge is to identify the cases in which the public provisions are directly addressed to the protection of competition, because in such case the same public framework provides the interpretative instruments useful in order to decode the loyalty principles which must lead the conduct of the entrepreneurs, in such a way that the violation of these provisions will represent an act of unfair competition. Should the public provisions not have the aim to protect competition, in such case, the conduct contrary to the public provisions may constitute an act of unfair competition pursuant to Article 2958 of the Italian Civil Code, but only if suitable to affect competition.

Furthermore, also this theory is immune from critics, given that, the most authoritative Italian doctrine, it appears *"proper to assume that, save in exceptional and duly justified circumstances, the violation of laws of the Member State is always in conflict with the principles of correctness"* [2]. Therefore, in or-

[1] This approach is criticized by C. Alvisi, *Concorrenza sleale, violazione di norme pubblicistiche e responsabilità*, 1997, p. 127, according to which in order to comply the unfair conduct with the breach of a mandatory rule the unfairness loses his autonomous legislative significance and represents a type of fault.

[2] For details see A. Vanzetti, V. Di Cataldo, *Manuale di Diritto Industriale*, 7ª ed., 2012.

der to discern the licit conducts from those illicit the infringed public provisions should first be distinguished depending on whether they provide restrictions to the business activity, costs or fees. In the event that the first category of provisions will be infringed, in this case a competitively illicit will occur. With regard to the possibility of an infringement of costs rules, the violation will consist in a complex legal matter which includes a competitive offence in the event that the violation is associated to a competitive damage. Lastly, where the infringement will regard fee provisions, even if the difficulty to see in this violation a competitive behavior has been invoked by various parties, this possibility cannot be excluded. In the same way as the infringement of costs rules (such as public employees' provisions), also the fees rule (such as license and authorizations) can lead to savings and in turn to a competitive advantage which, where taken, will cause a competitive damage.

As regards to the second case *ii)*, the question is where the compliance of a conduct with a public provision may facilitate an evaluation in terms of illegality: the answer, far from being unequivocal, involves different disciplines. In general terms, the compliance of a conduct with a provision, also if mandatory, does not automatically entail its compliance with a different legislative corpus. Furthermore, in order to establish the violation of competition law, one has to go back to the aim of the public provision, and only if this pursuits a competitive aim and the conduct realizes only that objective, it would seem reasonable to stop any other evaluation on the relevance of the conduct pursuant to Article 2598 of the Italian Civil Code.

2. Unfair competition and tort law

Against a behavior adopted by a company in breach of a public provision which, in light of the above evaluation, is also breaching competition law, the affected competitors or the relevant professional associations shall be entitled to protect their interests in the competent judicial offices and in particular to claim before the civil court: *i)* an action for an injunction and for removal of effects caused by the illicit conduct, for which is sufficient to provide only the evidence of the act of unfair competition, but not the misconduct or fraud of the infringer, and neither the actual economic damage, given that it is sufficient that the damage is potential; *ii)* an action for damages, for which it is necessary to provide the evidence of the subjective state of the infringer (misconduct that, in any case, is presumed if the act of unfair competition is verified) and of the financial loss.

In the course of this action the court may order the publication of the judgment in the press as a sanction.

Indeed, where the competitor believes that he has been affected by an act of unfair competition, he can take advantage, at least at the level of principle, of Article 2043 of the Italian Civil Code to safeguard its interests.

According to the case law, the relationship between the two provisions has been solved by considering the breach of competition law as a type of tort [3]. Particular attention is paid to the peculiarity of the unfair competition with respect to the tort, which should be identified by reference to the legitimacy (active and passive) requirements and also to the reaction capability against the violation; with regard to the conditions and compensations the two categories coincide [4]. In so doing, the Aquilian liability pursuant to art. 2043 of the Italian Civil Code plays a subsidiary role such that this provision is applied whenever there aren't the subjective and objective requirements for the implementation of Article 2598, n. 3 of the Italian Civil Code [5].

3. State aids provisions and unfair competition

In the light of the above framework, it is now appropriate to examine the existing relationship between the public provisions on State aids and the repressive rules on unfair competition, which promotes, as stated above, at private level, the protection of competition between companies which are competitors on the market [6].

The relationship between the beneficiary company and the Member State, on one side, and the relationship between the Member State that grants aid and the competitors of the beneficiary company, which in claiming the incompatibility or the unlawfulness of the measure request to the State the compensation for the damage caused by its concession, on the other side, remain outside the sphere of this analysis.

What is relevant to assess the existence of an unfair competition conduct before the court is the autonomous legal significance of the act of unfair competi-

[3] Cass., n. 1829, 26 June 1973, in *Foro it.*, 1973, I, c. 3371. See in the opposite sense, Cass, n. 2106, 6 July 1971, in *Riv. dir. comm.*, 1972, p. 108, according to which «the unfair competition remains an autonomous category and doesn't constitute a type of tort». See in doctrine, A. Genovese, *Il risarcimento del danno da illecito concorrenziale*, 2005, p. 23; C. Alvisi, *Concorrenza sleale, violazione di norme pubblicistiche e responsabilità*, 1997, p. 125.

[4] A. Genovese, *Il risarcimento del danno da illecito concorrenziale*, cit.

[5] For details see, A. Vanzetti, V. Di Cataldo, *Manuale di Diritto Industriale*, 7ª ed., 2012.

[6] See for an updated view on the pursued values, V. Falce, *Appunti in materia di disciplina comunitaria sulle pratiche commerciali sleali*, in *Riv. dir. comm.*, 2009, p. 423.

tion put in place by the company receiving State aid over a direct competitor, where the conduct is: *i)* fundamentally against the competition law and incompatible with State Aids framework, or direct to lead to specific commercial results due to the unfair exploitation of an aid [7], *ii)* directly or casually attributable to the aid received.

For the purposes of point *ii)* the question arises is evidentiary, since the competitor shall be required to prove the casual link between the measure criticized and the conduct that implies a breach of competition law, while for the purposes of point *i)* the starting point is that the rules on State Aids are directly and specifically designed to ensure that the competition between companies is not distorted by aids that unduly benefit some companies or some manufacturing over their competitors. Therefore, the above provisions provide the notion of professional correctness pursuant to Article 2598 of the Italian Civil Code, in such a way that the assessment of compliance between practice and State Aid provisions means the compliance of a conduct with the correctness paradigm.

2. *(Following) The liability of the beneficiary company receiving the aid towards its direct competitors.* – Even though it is debatable whether a company is obliged to verify the regularity and, in the last resort, the legality of the aid granted (all based on the assumption that the above obligation of notice and standstill have only vertical effects and so that are applicable exclusively to Member State [8]) the European case law rejects the suggestion that the beneficiary of an unlawful State Aid, according to the European Union law, may be held liable for the injury suffered by a competitor [9].

Disregarding the range of action of the general duty of care that lies with the *accipiens* [10], and the risk effectively run by the *accipiens* taking advantage of an

---

[7] A. Genovese, *Tutela urgente della concorrenza e inibitoria della condotta dell'impresa beneficiaria di aiuti di Stato*, in *Corr. giur.* 2007, 6, p. 845.

[8] C. Giust., 11 July 1996, *Syndicat français de l'Express international (SFEI) e a. c. La Poste e a.*, C-39/94, in *Racc.* 1996, I-3547. See in the opposite sense A. Saggio, *La responsabilità dello Stato per violazione del diritto comunitario*, in *Danno e* responsabilità, 2001, 3, 223, which criticized this approach considering it overly formalistic and capable to neglect the direct effect of the European Union law on individuals.

[9] C. Schepisi, *Aiuti di Stato e tutela giurisdizionale. Completezza e coerenza del sistema giurisdizionale dell'Unione europea ed effettività dei rimedi dinanzi al giudice nazionale*, Giappichelli, 2012.

[10] See F. Ferrero, *Risarcimento dei danni e aiuti di Stato alle imprese: recenti sviluppi*, in *La "Modernizzazione" della disciplina sugli aiuti di Stato. Il nuovo approccio della Commissione europea e i recenti sviluppi in materia di public e private enforcement*, (a cura di) C. Schepisi: according to the author to admit that a beneficiary of a State aid could ignore its unlawfulness or not compliance with respect to the European regulation is increasingly difficult, because of the presence of abundant case law and guidance acts which codified the use of the Courts and of the European Commission.

aid not previously notified and assessed favorable by the European Union, the possible future action for the unfair competition, filed by the competitor against the beneficiary, may follow not the European Union law (that is only relevant for the Member States), but rather the principles and requirement on liability set forth by the national law [11].

Therefore, the competitor can file the action pursuant to Article 2598 of the Italian Civil Code only where he is able to give evidence of the casual link between the unlawful measure and the unfair conduct carried out according to the measure (in the event of incompatible aid) or of the autonomous unfair conduct in breach of the Articles 101 and 102 of TFEU (or of the corresponding national provisions) or carried out in an illicit way [12] (in the event of unlawful aid), because the solution of the regulatory "coverage" given by the measure that grants an aid in breach of the European Union law can hardly be applicable and the related legitimate expectations by the beneficiary can be hardly laid down. In both the circumstances above, the national Court carries out a subsidiary and complementary function to the European Commission, as, in addition to several preliminary assessments, the Court is called upon to ascertain whether an adopted strategy not only is directly attributable to the aid granted, but also if this strategy has resulted in an act of unfair competition, which consequences has not been absorbed by the measures adopted to restore the *status quo ante* in terms of competition conditions on the market. Because of the need for coordination, in the event that the European Commission has not expressed an opinion on the compliance of the aid with the European Union law, the national Court shall be empowered to adopt, if so requested, the suitable protective measures. Lastly, if the national Court comes to a conclusion about the compliance of the aid after the European Commission, must necessarily take into consideration the European Commission's decision.

Moving on the issue of whether the realized conduct results in compliance with the State aid provisions (as legitimate because it has been notified regularly to the European Commission, and compatible because it has been authorized by the European Commission) but, is however unfair pursuant to Article 2598 of the Italian Civil Code, the procedural compliance – which since doesn't imply any assessment on the merits, doesn't ensure the compliance of the company's conduct on the market with the competition law – needs to be distinguished

[11] Court of Justice, "SFEI", cit; European Commission, Commission notice on the enforcement of State aid law by national courts, in Official Journal of the European Union, 2009, C-85 11, § 44 e 53. In doctrine, please see, C. Schepisi, *Aiuti di Stato e tutela giurisdizionale*, cit.; A. Genovese, *Tutela urgente della concorrenza e inibitoria della condotta dell'impresa beneficiaria di aiuti di Stato*, cit.

[12] C. Schepisi, *Aiuti di Stato e tutela giurisdizionale*, cit.

from substantial compliance, which can lead to a concurrence of provisions. In this event, the assessment of the national Court, that must take as a basis the regulatory framework and take into account the primacy of the European law over national law, cannot assess the implementation of the benefit derived by the State aid and the conducts that are required by the beneficiary of the measure, as contrary to the principle of professional correctness, because, within these limits, the safeguard of competition and correctness is ensured by the European provisions on State Aids.

Conversely, the national Court outside of this area can freely assess the correctness of the conduct pursuant to Article 2598 of the Italian Civil Code [13] and where appropriate the Court can use the instruments of private enforcement. This, on the assumption that the *accipiens* has a privileged position from which derives the special responsibility of not exploit the competitive advantage granted over the limits, margins, aims permitted causing a further and unjustified damage to the market and to the competitors.

4. Evolution of the case law

The abundant case law on State aid matter has rarely worked on interferences and intersections with the repressive rules on unfair competition [14]. The main cases which signed the evolution are the following:

Grandi Traghetti di Navigazione Case

In this case Grande Traghetti di Navigazione (hereinafter GTN) claimed Viamare di Navigazione (hereinafter VDN) before the Court of Genoa arguing its unfair behavior consisted in the application of tariffs below-costs and unfair customer solicitation. GTN in particular argued that the application of tariffs below-costs for the navigation services from Genoa to Termini Imerese was not the result of an autonomous business policy, but was the immediate and direct result of the State aid granted by the Italian Government to Finmare, parent company of VDN. For this reasons GTN asked to the Court the adoption of a protective measure towards VDN pursuant to Article 700 of the Italian civil procedural code, and sought a preliminary ruling from the Court of Justice in

[13] A. Genovese, *Tutela urgente della concorrenza e inibitoria della condotta dell'impresa beneficiaria di aiuti di Stato*, cit.

[14] The case law shows that the actions filed by the beneficiary to oppose to an internal execution order are far more numerous than those carr*ied out by the competitor based on the mere illegality of the aid, or than those which follows a negative decision by the Commission*. For details see C. Schepisi, *Aiuti di Stato e tutela giurisdizionale*, cit., p. 206.

order to assess whether the State measures in question could be considered as State aid with reference to the relevant legislation.

The Court of Genoa has recognized, in principle, that a State aid that infringes the European regulation represents an act of unfair competition, with the result that the beneficiary may be concerned by a protective measure. However, the Court of Genova in the merit of the case excluded the application of State aid rules as regards the navigation services (see Reg. EC 3577/92, art. 6) and secondarily denied that the financing granted to VDN could constitute State aid because were resources raised on the market.

Alitalia/Airone Case [15]

In this case, the European Commission in 2004 authorized, as a form of individual aid from the Italian State to the national Italian airline, the provision of a guarantee for the bridge loan granted by several credit institutions to Alitalia in March 2005 for a period of twelve months in order to ensure the coverage of the cash requirements and avoid the risk of insolvency for the company. The European Commission had considered the aid in compliance with the European regulation provided that two conditions were met: *i)* that the delivery of the aid was related to the adoption of a suitable restructuring plan and *ii)* that during the granting of aid was avoided an increase of capacity of the Alitalia fleet. In November 2005, Alitalia had expressed its interest in participating to a tender procedure for the acquisition of the Volare Group under special administration. Airone, also interested in the procedure had asked to the Court of Rome to inhibit, as a precautionary measure, the participation of Alitalia arguing that the Italian airline would use the competitive advantages of the aid for aims different from those inherent to the aid granted. By order dated January 27th, 2006, the Court of Rome had embraced the Airone's position in the belief that on the date of the expression of its interest Alitalia benefited of the aid, which was granted to ensure only the functioning of the company and not also the increase of capacity of the fleet.

Alitalia had claimed against the decision of the first instance court and the Court, assessed the facts and the arguments, had upheld the complaint and revoked the precautionary measure. According to the Court, Alitalia before returning the bridge loan had only expressed its interest in participating to the tender for the acquisition of the company unit on sale. Alitalia had only realized a preliminary and preparatory conduct that was inappropriate to affect the functioning of the market, the competitors and the results of the procedure until the irrevocable purchase offer, that was then released on December 2005, and so

[15] Court of Rome, Order 27 January 2006 and Court of Rome, sez. II, Order 14 March 2006.

after the recapitalization and the (early) reimbursement of the bridge loan. In other words, Alitalia had released the irrevocable purchase offer after the termination of the efficiency of the State aid and so of the commitment of Alitalia toward the European Commission to don't increase the fleet. To conclude, the Court had denied the existence of the *fumus boni iuris* in the claim of Airone because, considered the timing of facts and acts, Alitalia had not disregarded the European regulation on State aids and had not implemented any act of unfair competition.

This case has been the subject to doctrine criticisms [16] because in the first order the Court applied the cumulation of liabilities criteria without having assessed incidentally the violation of any European requirement and without a motivated opinion on the anti-competitive consequences of Alitalia's conduct in a well-identified market.

The order that decided on the action brought by Alitalia, on the other hand, based its decision on the legal and property consequences of the conduct of Alitalia, without taking into account the restrictive effects deriving from the business strategy of the company. Otherwise, the Court should have first and foremost identified the limits to the conduct of Alitalia imposed by the Commission decision which authorized the aid, and subsequently the Court should have assessed the lawfulness of the conduct realized with respect to the more rigid requirements of the competition law. From this point of view might have been argued that the relevant market was affected, in competition terms, by the presence of aid to a company but at the same time was protected by initiatives of the beneficiary company that amplified the distortive effects of the aid. Following this orientation, the Alitalia conduct could have been considered, notwithstanding the fact that is complying with the State aid rules, unfair and suitable, likely to harm competitors and therefore detrimental to the repressive rules of unfair competition.

Traghetti del Mediterraneo Case [17]

In this case, Fallimento Traghetti del Mediterraneo claimed the company Tirrenia Navigazione, a competitor on the maritime services market in Sicily and Sardinia, for having carried out conducts as unfair as realized as a consequence of the State aid granted under the law 684/74 which would have allowed the company to apply prices below cost. The claim, rejected by the Court of Naples and, subsequently, by the Court of Appeal, has been filed before the Su-

[16] A. Genovese, cit.

[17] Cass., n. 5087, 19 April 2000, Fallimenti Traghetti Mediterraneo S.p.A. c. Tirrenia di Navigazione S.p.A.

preme Court of Cassation which, confirming the correctness of the decisions of the Courts of merit, emphasized that: *i)* the State aid is, in principle, prohibited because not in compliance with competition law; *ii)* the distortive effect generated by the State aid is irrelevant in the assessment of the compatibility of the state measure with the European regulation as this effect is an essential component of the aids and shall be admissible if it is directed to the protection of interests that would not otherwise find satisfaction [18]. In this case, the Supreme Cassation Court stated that the tariffs applied by Tirrenia were not the expression of their own business decisions, but represented the implementation of a specific national regulation and, for this reason, there was no autonomy to constitute an act of unfair competition.

5. Conclusions

The exploration of the areas of intersections and interferences between the rules on aid and the provisions of competition law leads to a wider question, such as whether, when and under what conditions the breach of the public provision in general and in particular the ones on aid constitutes an act of unfair competition, independently regrettable pursuant to and for the purposes of Article 2598 of the Italian Civil Code. If, in legal point, the private enforcement road, aimed at outline an unfair behavior, is open to use every time that the beneficiary undertaking exploits the competitive advantages achieved beyond the aim in respect of which and for the time within the measure is granted, or with exorbitant, excessive and disproportionate methods, on the other hand, in point of fact, the evidence of the illicit and its autonomous relevance is very hard, thus drastically restricting not only the number of actions filed but above all the chance of success.

[18] For a critical remark of the judgment please see L. Arnaudo, *Aiuti di Stato, tariffe e concorrenza: tra competenze chiuse e questioni aperte*, in *Riv. it. dir. pubbl. com.*, 2000, 6, p. 1368.

IL DATA PROTECTION OFFICER: LE CARATTERISTICHE E I CONNESSI PROFILI DI RESPONSABILITÀ

Maria Roberta Perugini e Deborah Caputo

Abstract:

Premesso un breve inquadramento del concreto ruolo e dell'effettiva funzione del Data Protection Officer (DPO), l'articolo analizza i diversi profili di responsabilità (privacy e civilistici) di tale figura in relazione ai trattamenti dell'ente designante (senza però tralasciare alcune riflessioni sui trattamenti che il DPO attua "autonomamente" nel contesto dell'esercizio delle proprie funzioni). In particolare, l'analisi viene condotta prendendo in considerazione due possibili situazioni "patologiche" (e precisamente, inadempimento e conflitto di interessi), evidenziando al contempo le peculiarità ravvisabili a seconda che il DPO sia interno (in quanto dipendente dell'ente designante) o esterno (in quanto consulente incaricato in forza di un contratto di servizi).

Key-words: DPO, Responsabilità

Summary: Introduzione. – 1. Ruolo e funzione del DPO. – 2. Le caratteristiche essenziali del DPO. – 3. Assenza di responsabilità "esterna" del DPO per i trattamenti dell'ente designante e per i trattamenti attuati nell'esercizio delle proprie funzioni. – 4. Responsabilità del DPO per inadempimento: inquadramento del tema – (*Segue*). Responsabilità del DPO per inadempimento: principi applicabili. – 5. Obbligo dell'ente designante di "sostenere" il DPO e conseguenze in tema di allocazione di responsabilità tra designante e DPO. – 6. Profili di responsabilità in caso di DPO in conflitto di interessi: inquadramento. – 7. DPO interno in conflitto di interessi: azioni di prevenzione. – 8. Responsabilità dell'ente per il conflitto di interessi del DPO interno. – 9. DPO esterno in conflitto di interessi: azioni di prevenzione. – 10. Conseguenze del conflitto di interessi in termini di allocazione della responsabilità tra designante e DPO. – 11. Effetti del conflitto di interessi sul contratto di servizi tra privati. – 12. Responsabilità del DPO in conflitto di interesse nominato attraverso gara pubblica.

Introduzione

L'introduzione con il Reg. UE 679/2016 (GDPR) del *Data Protection Officer* (DPO) ha sinora portato in Italia all'adozione di soluzioni perlopiù di

compromesso, poco rispondenti alla normativa o addirittura manifestamente inadempienti sotto diversi profili: conflitti di interesse, incompetenza, assegnazione di mezzi e tempi insufficienti conducono allo svuotamento sostanziale di questo strumento, riducendo l'atto di nomina a mero adempimento formale e dunque al fallimento – sotto questo profilo – del percorso di conformità alle norme del titolare o responsabile del trattamento che si dota del DPO.

Per comprendere l'effettiva portata e le conseguenze di tale mancata conformità è necessario inquadrare la funzione assolta dal DPO nel contesto delle attività di trattamento dell'ente designante e del relativo percorso di *accountability* e, al contempo, individuare le caratteristiche essenziali di questa figura.

In quest'ottica, è utile ricordare che il sistema complessivo introdotto dal GDPR fa perno sulla prevenzione del rischio di violazione di dati personali e dei (connessi) diritti e libertà fondamentali della persona. Affinché tale prevenzione sia adeguata ed efficace, il GDPR ha attribuito ai soggetti attivi del trattamento compiti e obiettivi generali (quali la progettazione, l'attuazione e il controllo del trattamento) e, al contempo, la capacità (e l'onere) di dimostrare che il trattamento attuato è conforme alle norme (art. 5, co. 2 e 25 GDPR): in tale modo è stato procedimentalizzato, in capo a detti soggetti, un principio generale di responsabilità (art. 24 GDPR: l'"*accountability*").

Un siffatto sistema induce l'ente ad adottare misure concrete per "*attuare i principi di protezione dei dati*" (art. 25 – Privacy by design e by default) e "*garantire un livello di sicurezza adeguato al rischio*" (art. 32 – Sicurezza del trattamento), in modo da offrire nella pratica una protezione che sia reale ed effettiva.

Naturalmente, affinché le misure adottate risultino efficaci è necessario che vengano individuate dall'ente autonomamente, in rapporto alle peculiarità del caso specifico, ponendo particolare attenzione al rischio inerente al trattamento e alla natura dei dati da proteggere.

Nel contesto dell'elaborazione, da parte del titolare del trattamento, di un sistema di gestione *privacy* idoneo a minimizzare il rischio, assume pertanto grande rilevanza la nomina (anche volontaria) del DPO, il quale viene a rappresentare un vero e proprio strumento dell'*accountability*, adottabile (obbligatoriamente o volontariamente, a seconda dei casi) dall'ente nel contesto delle azioni volte ad attenuare il rischio di violazione dei dati personali e dei diritti delle persone fisiche.

1. Ruolo e funzione del DPO

Il DPO si configura quale terzo rispetto al titolare o responsabile del trattamento che lo designa: è lo specifico organismo istituito dal GDPR cui è attribui-

to il compito di assistere il titolare/responsabile del trattamento «*nel controllo del rispetto del (...) regolamento*» [1] e che per legge deve svolgere la propria funzione (mista di consulenza, vigilanza e controllo) in assoluta autonomia e indipendenza [2].

È inoltre compito del DPO fungere da interlocutore dell'Autorità Garante e degli interessati per l'ente designante [3] (e «*sorvegliare l'osservanza*» di tutte le norme nonché delle politiche del designante in ordine al trattamento dei dati personali, «*compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*» [4]).

Il DPO è dunque chiamato ad assumere un ruolo chiave nella definizione del percorso di conformità al GDPR dell'ente designante. Ciò malgrado, esso è estraneo al trattamento dell'ente sotto il profilo decisionale e della responsabilità che ne deriva (profili rimessi dalla legge esclusivamente al titolare e al responsabile del trattamento, come si preciserà tra breve).

Si tratta, infatti, di una figura di natura eterogenea rispetto al titolare e al responsabile – in rapporto ai quali si colloca non in posizione alternativa o cumulativa, ma *a latere* –, non rivestendo alcun diretto ruolo attivo nei relativi trattamenti, pur assumendo in rapporto ad essi un fondamentale valore strategico.

---

[1] V. considerando 97 GDPR: «per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente».

[2] V. spec. art. 38, par. 3 e 6, GDPR.

[3] V. artt. 38, par., e art. 39 GDPR.

[4] V. art. 39, par.1 lett. b, GDPR.

2. Le caratteristiche essenziali del DPO

In ragione della complessità del ruolo e delle funzioni attribuitegli, il DPO dovrebbe: *i)* essere un professionista esperto, dotato di competenze specifiche e specialistiche in materia di protezione dei dati personali, con particolare riferimento alla conoscenza della normativa e delle prassi inerenti [5]; *ii)* possedere essenziali requisiti di indipendenza [6]; *iii)* essere collocato, nel contesto aziendale dell'ente designante, in una posizione tale da riferire al più alto livello gerarchico [7] e da non dare adito a un conflitto di interessi [8].

Le peculiarità che caratterizzano la figura in esame inducono ad alcune riflessioni sui profili di responsabilità che ne scaturiscono.

3. Assenza di responsabilità "esterna" del DPO per i trattamenti dell'ente designante e per i trattamenti attuati nell'esercizio delle proprie funzioni

È innanzitutto necessario chiedersi, da un lato, perché all'autonomia ed indipendenza del DPO nello svolgimento della propria funzione non conseguano responsabilità autonome "esterne" per sanzioni o a titolo di risarcimento dei danni agli interessati, a fronte di una eventuale non conformità alla legge dei trattamenti dell'ente designante; dall'altro lato, se possano individuarsi a carico del DPO – e in che termini e con quali conseguenze – profili di responsabilità "interna", dunque nei confronti dell'ente designante.

Partendo dal primo interrogativo, è un dato di fatto che le conseguenze del

---

[5] V. art. 37, par. 5, GDPR.

[6] V. considerando 97: "(…) Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

[7] V. art. 38, paragrafo 3, GDPR: «Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». A tale proposito, si ricorda che il "vertice gerarchico" è stato identificato in linea generale dal WP29, nelle proprie "Linee-guida sui responsabili della protezione dei dati (RPD)", [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048] nel CdA: «Al riguardo, l'art. 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che **il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni** e delle raccomandazioni fornite dal RPD nel quadro delle sue funzioni di informazione e consulenza a favore del titolare o del responsabile.» (cfr. par. 3.3. «Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente»)

[8] V. art. 38, par.6, GDPR.

fallimento dell'ente designante nel relativo percorso di conformità al GDPR ricadono esclusivamente su di esso: infatti, l'art. 83 GDPR prevede sanzioni solo a carico del «*titolare*» e del «*responsabile*» del trattamento mentre non se ne rinvengono rivolte al DPO; parimenti, l'art. 82 GDPR riconduce espressamente la responsabilità per il risarcimento del danno causato da una violazione del GDPR ai soli «*titolare*» e «*responsabile*» del trattamento.

È importante indagare la *ratio* di tale scelta legislativa.

Va considerato che l'ente designante persegue proprie finalità generali di gestione aziendale/istituzionale che comprendono – presupponendolo – il rispetto delle norme applicabili, tra cui l'adempimento dell'obbligo di *conformità* al GDPR: proprio in osservanza di tale obbligo è dovere dell'ente esplicitare in un apposito incarico i compiti assegnati al DPO [9] e fornirgli «*le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*» [10].

Tuttavia in questo contesto, seppure nei limiti fissati dai compiti predefiniti nell'incarico, il DPO determina ed effettua in «*autonomia e indipendenza*», obbligatoriamente in assenza di qualsivoglia «*istruzione*» [11], i trattamenti di dati personali strettamente connessi all'esercizio delle sue funzioni, e dunque per specifiche finalità di assistenza dell'ente e controllo della relativa conformità al GDPR.

Ciò detto, sembrerebbe naturale desumere in capo al DPO una titolarità di tali trattamenti [12], seppure caratterizzata da una evidente correlazione con i trattamenti direttamente imputabili all'ente e finalizzati alla conformità normativa della propria azione, in generale e con specifico riferimento al GDPR.

Va però sottolineato che la stretta correlazione funzionale esistente tra la finalità particolare dei trattamenti effettuati dal DPO e quella generale di conformità alla legge perseguita dell'ente designante è istituita dalla stessa normativa [13], con la conseguenza che la prima appare essere (non altro che) una subfinalità della seconda.

---

[9] V. art. 39 GDPR.

[10] V. art. 38, par. 2, GDPR.

[11] V. art. 38, par. 3 GDPR.

[12] Non vi è difficoltà ad individuare la titolarità del trattamento in capo ad un organo interno di un ente: l'art. 4, n.1 GDPR definisce infatti il «Titolare» quale «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Dunque, il presupposto qualificante della titolarità è solo il potere decisionale esercitato nella determinazione dei trattamenti.

[13] Tale correlazione è ben riassunta dal dettato del già citato Considerando 97: «il titolare del trattamento o il responsabile del trattamento **dovrebbe essere assistito** da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento».

Insomma, la finalità dei trattamenti del DPO è una specificazione di quella generale propria dell'ente stesso (vale a dire, l'adempimento da parte di quest'ultimo dell'obbligo legale di *conformità* al GDPR), che è il solo che ha il potere decisionale sui mezzi per raggiungerla: innanzitutto – nei casi di istituzione volontaria – la stessa decisione di dotarsi del DPO (e se questo debba essere "interno" o "esterno"), poi la definizione dell'ampiezza del relativo incarico, delle iniziative per garantirne indipendenza e autonomia nello svolgimento delle relative funzioni, delle risorse da stanziare, nonché l'istituzione e la regolamentazione dei flussi informativi tra DPO e altri organi / funzioni aziendali, l'adozione di misure di sicurezza tecniche ed organizzative, etc.

Ne discende che il DPO non è soggetto attivo autonomo neppure dei trattamenti da esso attuati nello svolgimento del proprio ruolo; tali trattamenti, infatti, sono imputabili direttamente all'*accountability* dell'ente di riferimento, cui in ultima analisi sono rimesse le decisioni in ordine alle relative finalità e modalità.

L'articolazione dell'incarico da parte del titolare/responsabile diventa così il punto di snodo per il coordinamento tra l'autonomia e indipendenza della funzione di vigilanza rispetto al soggetto vigilato e la necessaria riconducibilità delle attività di trattamento svolte dal DPO nell'alveo di quelle proprie dell'ente designante.

Pertanto, il DPO non assume alcuna diretta responsabilità né per sanzioni né per risarcimenti nei confronti degli interessati per la non conformità dell'ente di riferimento alle norme (neppure se gli inadempimenti sono dipesi da colpa o dolo del DPO).

Parimenti, ricade integralmente sull'ente designante l'obbligo di informare tutti i potenziali interessati della nomina del DPO e dei trattamenti ad esso attribuiti, indubbiamente connessi alle funzioni previste dalla legge [14], in aggiunta alla obbligatoria pubblicazione dei dati del DPO.

4. Responsabilità del DPO per inadempimento: inquadramento del tema

Se il DPO va esente da responsabilità in termini di sanzioni applicabili nel caso di irregolarità o inadempienze agli obblighi in materia di protezione dei dati personali, sotto il profilo della responsabilità "interna" la prospettiva invece appare differente, considerato che: *(i)* tra ente designante e DPO sussiste un rapporto contrattuale; *(ii)* come precisato, per previsione di legge il DPO deve essere un soggetto dotato di competenze specifiche e *conoscenze specialistiche* della materia.

[14] Spec. art. 39 par. 1 lett. b) e c) GDPR.

Occorre pertanto indagare cosa accade nell'ipotesi in cui il DPO svolga i propri compiti senza diligenza, ad esempio fornendo al titolare informazioni e consigli non corretti in merito all'adempimento delle prescrizioni a suo carico o pareri erronei sulla valutazione d'impatto.

La questione va affrontata tenendo in debita considerazione il dovere del designante di "sostenere" il DPO «*nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*» [15].

La normativa non effettua distinzioni tra DPO interno o esterno in merito alle modalità e al tenore del sostegno che il designante è tenuto ad offrire. Tuttavia, per esplorare compiutamente le possibili responsabilità del DPO in caso di sua negligenza o imperizia è necessario distinguere il caso del DPO dipendente da quello del DPO esterno, e ciò sia in relazione al livello di diligenza richiesto sia al contenuto dell'obbligo di sostegno gravante a carico del designante.

(*Segue*). Responsabilità del DPO per inadempimento: princìpi applicabili

Con riferimento al DPO "esterno" si ricorda che, in via generale, i parametri di diligenza sanciti dalla legge per valutare la condotta del debitore di una prestazione sono previsti dall'art. 1176 c.c. («*Diligenza nell'adempimento*»), che introduce due parametri: uno generico al primo comma («*Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia*») e l'altro specifico/qualificato al secondo comma («*Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata*»).

In base alla norma citata la condotta del professionista, in ragione delle sue competenze specialistiche, deve essere valutata assumendo come criterio di confronto la preparazione, il possesso di nozioni tecniche e l'attenzione (vale a dire l'accuratezza, la prudenza e la precisione) media che quella determinata professione richiede [16].

---

[15] V. art. 38 par. 2 GDPR.

[16] Sul punto, v. C.M. Bianca, in *Diritto civile*, IV, *L'obbligazione*, Milano, 91. L'Autore definisce la «la diligenza adeguata alla natura dell'attività esercitata» che il debitore deve usare nell'adempimento delle obbligazioni professionali in luogo della diligenza del buon padre di famiglia richiesta per le prestazioni comuni, come «quello sforzo di energie e mezzi mediamente e normalmente richiesto alla categoria professionale a cui il debitore appartiene, che «esprime (...) una misura oggettiva dello sforzo volitivo e tecnico richiesto al debitore». Inoltre, secondo l'Au-

Nel caso del DPO troverà pertanto applicazione il parametro della diligenza professionale di cui al secondo comma dell'art. 1176 c.c., la cui mancata integrazione determina in capo al professionista una responsabilità anche per colpa lieve [17].

---

tore, «la diligenza professionale opera come criterio fondamentale di responsabilità e come criterio di determinazione della prestazione dovuta indicando nel primo caso, lo sforzo che il debitore deve impiegare per evitare l'inadempimento o l'inesattezza dell'inadempimento e, nel secondo caso, il modello di precisione e di abilita tecnica cui il comportamento dovuto deve conformarsi». Si veda anche A. Perullo, *Il lavoro autonomo*, in *Trattato di diritto civile e commerciale diretto da Cicu e Messineo*, XXVII, t. 1, Milano 1996, p. 580 ss., che ritiene che il dovere di attenzione si rapporti sempre con quello «medio» di una determinata categoria professionale di appartenenza, dovendosi intendere tale diligenza come buona, sebbene non eccezionale, ossia come diligenza qualificata. In giurisprudenza si afferma che, «il prestatore d'opera intellettuale viola il proprio dovere di diligenza, e perciò è inadempiente alle obbligazioni nascenti dal contratto d'opera professionale, quando risulti che agli abbia agito con negligenza, imperizia, imprudenza tali da violare le regole di comportamento alle quali si sarebbe attenuto un ipotetico professionista medio in relazione al caso concreto ed al risultato che le parti si ripromettevano». In giurisprudenza, per la giurisprudenza di merito v. Tribunale Bergamo, 12 marzo 2019, in Pluris, che (pronunciandosi sulla diligenza del professionista avvocato) ha avuto modo di precisare, in termini generali, che il professionista incaricato «nell'espletare la sua attività, deve impiegare la diligenza del professionista di media attenzione e preparazione ex *art. 1176 c.c.*»; Trib. Oristano, 29 novembre 2016, in Pluris che ha precisato che «l'inadempimento del professionista (che nella fattispecie era un avvocato) non può essere desunto senz'altro dal mancato raggiungimento del risultato utile avuto di mira dal cliente, ma deve essere valutato alla stregua della violazione dei doveri inerenti allo svolgimento dell'attività professionale e, in particolare, al dovere di diligenza. Quest'ultimo – trovando applicazione in subiecta materia il parametro della diligenza professionale fissato *dall'art. 1176, secondo comma, c.c.*, in luogo del criterio generale della diligenza del buon padre di famiglia – deve essere commisurato alla natura dell'attività esercitata, sicché **la diligenza che il professionista deve impiegare, nello svolgimento dell'attività professionale in favore del cliente, è quella media, cioè la diligenza posta nell'esercizio della propria attività dal professionista di preparazione professionale e di attenzione media**». Per la giurisprudenza di legittimità v, tra le altre, Cass, 20 novembre 2018, n. 29846, in *Pluris*. La Suprema Corte ha precisato che «le obbligazioni inerenti all'esercizio dell'attività professionale sono, di regola, obbligazioni di mezzi e non di risultato, in quanto il professionista, assumendo l'incarico, si impegna a prestare la propria opera per raggiungere il risultato desiderato, ma non a conseguirlo. Pertanto, ai fini del giudizio di responsabilità nei confronti del professionista, rilevano le modalità di svolgimento della sua attività in relazione al parametro della diligenza fissato *dall'art. 1176 c.c.*, comma 2, che è quello della diligenza del professionista di media attenzione e preparazione in relazione alla prestazione resa".

[17] Sul punto v. App. Milano, 5 aprile 2017, in Boll. Trib., 2017, 23, 1760, che ha precisato che «la diligenza che il professionista deve impiegare nello svolgimento della sua attività è quella media relativa al collega di preparazione professionale e di attenzione medie. La conseguente responsabilità può, quindi, trovare fondamento in una gamma di atteggiamenti subiettivi, che vanno dalla semplice **colpa lieve**, al dolo»; Trib. Monza, 18 settembre 2014, in Pluris, che ha espressamente affermato che «il professionista è tenuto ad eseguire la prestazione con la diligenza e la perizia adeguate alla materia tecnica di competenza (*art. 1176, comma 2, c.c.*) e risponde, in mancanza, anche per colpa lieve.». Per la giurisprudenza di legittimità v. Cass., 24 novembre 2003, n. 17871, in *Mass. Giur. It.*, 2003: la Suprema Corte ha confermato il principio per cui «in materia

Al contempo è importante segnalare, accanto alla norma generale (e in un certo senso ad "integrazione" [18] della stessa), l'art. 2236 c.c., che delimita la responsabilità professionale alle sole ipotesi di dolo o colpa grave quando la prestazione comporta la risoluzione di problemi tecnici di particolare complessità (vale a dire di problemi che trascendono la preparazione media) o novità [19].

La limitazione di responsabilità di cui all'art. 2236 c.c. è però circoscritta solo ai casi di imperizia giustificata dalla particolare difficoltà dei problemi tecnici affrontati, mentre non trova applicazione nei casi di negligenza e imprudenza, nei quali il professionista – essendo sempre operante il livello "alto" di diligenza richiestogli – risponde anche per colpa lieve [20].

Considerata la novità della figura del DPO e la complessità della normativa

---

di esercizio di attività professionale, il professionista è responsabile anche per colpa lieve (*art. 1176, secondo comma, c.c.*), salvo che la prestazione dedotta in contratto implichi la soluzione di problemi tecnici di speciale difficoltà…».

[18] Come precisato dalla giurisprudenza. Si veda, per tutte, Cass., 15 gennaio 2001, n. 499, in *Mass. Giur. It.*, 200.

[19] In tale senso, tra le tante, v. per la giurisprudenza di legittimità Cass., 22 aprile 2005, n. 8546, in *CD* Cedam 2005. La Suprema Corte ha affermato il condiviso principio per cui qualora la prestazione professionale implichi la soluzione di problemi tecnici di particolare difficoltà trova applicazione l'art. 2236 c.c. che prevede una attenuazione della normale responsabilità, nel senso che il professionista è tenuto al risarcimento del danno unicamente per dolo o colpa grave; per la giurisprudenza di merito, cfr. App. Milano, 5 aprile 2017, cit., che ha confermato il principio per cui «qualora la prestazione professionale da eseguire in concreto involga la soluzione di problemi tecnici di particolare difficoltà, la responsabilità deve ritenersi attenuata, configurandosi, secondo l'espresso disposto *dell'art. 2236 c.c.*, solo nel caso di dolo o colpa grave».

[20] In tale senso, si vedano: Cass., 27 ottobre 2011, n. 22398, in *Resp. civ.*, 2011, 12, 860, che ha precisato che, qualora l'inosservanza (che nella fattispecie consisteva nell'inosservanza da parte di un notaio dell'obbligo di espletare la visura dei registri immobiliari in occasione di una compravendita immobiliare) non sia riconducibile a un'ipotesi di imperizia ma a negligenza o imprudenza, «cioè alla violazione del dovere della normale diligenza professionale media esigibile ai sensi del secondo comma dell'art. 1176 c.c.», rileva anche la colpa lieve, non trovando applicazione «la limitazione di responsabilità prevista per il professionista dall'art. 2236 c.c. con riferimento al caso di prestazione implicante la soluzione di problemi tecnici di speciale difficoltà»; Cass., 13 marzo 2007, n. 5846 in *Ragiusan*, 2007, 281-282, 289, che ha affermato in termini generali che «*l'art. 2236 c.c.* (che nei casi di prestazione che implichino la soluzione di problemi tecnici particolarmente difficili, limita la responsabilità del professionista ai soli casi di dolo o colpa grave) non trova applicazione per i danni ricollegabili a negligenza o imprudenza, dei quali il professionista risponde anche solo per colpa lieve. Infatti l'applicazione *dell'art. 2236 c.c.* è circoscritto ai casi di imperizia ricollegabili alla particolare difficoltà di problemi tecnici che l'attività professionale in concreto renda necessario affrontare»; Cass., 19 aprile 2006, n. 9085 in *Mass. Giur. It.*, 2006, che ha osservato che la «limitazione di responsabilità professionale (…) ai soli casi di dolo o colpa grave, ai sensi *dell'art. 2236 c.c.*, attiene esclusivamente alla perizia, per la soluzione di problemi tecnici di particolare difficoltà, con esclusione dell'imprudenza e della negligenza. Infatti anche nei casi di speciale difficoltà, tale limitazione non sussiste con riferimento ai danni causati per negligenza o imprudenza, dei quali [il professionista] risponde in ogni caso».

in materia di protezione dei dati personali, è tutt'altro che da escludere l'applicabilità di tale disposizione per valutare un'eventuale responsabilità del DPO per imperizia.

Passando al caso del DPO "interno", ossia dipendente del designante, per la definizione della sua responsabilità per inadempimento rilevano, oltre ai criteri generali di diligenza già esaminati (art. 1176 c.c.), anche le norme specificamente dettate per i lavoratori subordinati e precisamente l'art. 2104 c.c. («*Diligenza del prestatore di lavoro*»), in forza del quale: «*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale*».

Sul piano generale, il parametro della diligenza (insieme al criterio dell'osservanza) specifica il contenuto della prestazione di lavoro subordinato e costituisce indice di misura dell'adempimento della prestazione [21], concorrendo a individuare i doveri del lavoratore [22].

Quanto all'intensità della diligenza richiesta, è pacifico in giurisprudenza che l'obbligo di diligenza del lavoratore subordinato debba essere letto con maggiore intensità in ragione della sua qualifica professionale e che quindi varî a seconda della delicatezza e complessità delle mansioni affidate [23].

Da ciò discende che anche l'attività del DPO dipendente deve essere valutata ai sensi del secondo comma dell'art. 1176 c.c., e dunque in forza del criterio di diligenza qualificata.

Ciò ben si concilia con la prospettazione che il GDPR offre di questa nuova figura, quale soggetto dotato di competenze specifiche e qualificate, e con il tenore dell'art. 2104 c.c., che costituisce una specificazione del principio generale stabilito dall'art. 1176 c.c.

Da queste considerazioni emerge che in linea di principio, in caso di prestazione non conforme agli standard professionali di riferimento, il DPO inadempiente all'obbligo di diligenza (nascente dal contratto di lavoro o di servizi) si espone a responsabilità contrattuale *ex* art. 1218 c.c.: il DPO potrà quindi essere chiamato a risarcire il designante dei danni da quest'ultimo subìti per colpa della sua condotta negligente (si pensi, ad esempio, all'inflizione di una sanzione

---

[21] In tale senso v. Galantino, in *Diritto del lavoro*, Torino, 1998, 452.

[22] In tale senso v. F. Carinci, R. De Luca Tamajo, P. Tosi, T. Treu, in *Diritto del lavoro*, II, *Il rapporto di lavoro subordinato*, Torino, 1998, 236.

[23] Sul punto, v., per la giurisprudenza di legittimità, Cass., Sez. Lavoro, 9 ottobre 2013, n. 22965, in *Danno e Resp.*, 2014, 2, 216; Cass., 15 marzo 1977, n. 1037, in *Pluris*; per la giurisprudenza di merito, Trib. Milano, 6 luglio 1996, in *Lavoro nella Giur.*, 1996, 1032. In dottrina, v. F. Santoni, in *Rapporti speciali di lavoro, Il licenziamento discriminatorio del dirigente*, Torino, 1993, 122, secondo il quale la delicatezza delle funzioni dirigenziali esige una diligenza più intensa, da apprezzarsi in relazione allo specifico contenuto del rapporto ed alle mansioni contrattualmente dovute dal prestatore il quale rivesta la qualifica di dirigente.

da parte del Garante, a un eventuale risarcimento corrisposto dal designante all'interessato per errori imputabili al DPO, nonché al danno reputazionale conseguente a certi tipi di *data breach*).

Assume inoltre rilievo nel (solo) caso del DPO "interno" anche una eventuale responsabilità disciplinare [24].

Secondo l'orientamento prevalente della giurisprudenza di legittimità [25], in caso di danni procurati dal lavoratore al datore di lavoro, quest'ultimo in linea generale può chiedere il risarcimento dei danni, avviare il procedimento disciplinare o procedere con entrambi contemporaneamente (sempre che il contratto collettivo di lavoro applicabile alla fattispecie concreta non stabilisca condizioni più restrittive per il datore, ad esempio prevedendo che esso possa chiedere l'indennizzo solo dopo avere adottato il provvedimento disciplinare nei confronti del dipendente negligente).

5. Obbligo dell'ente designante di "sostenere" il DPO e conseguenze in tema di allocazione di responsabilità tra designante e DPO

Appurato che il DPO inadempiente al contratto si espone nei confronti del designante a una responsabilità risarcitoria, è utile svolgere qualche considerazione di carattere pratico in merito al più volte citato "sostegno" del designante, il cui contenuto può influenzare in modo decisivo l'allocazione della responsabilità eventualmente contestata al DPO.

Nella generalità della lettera dell'art. 38 par. 2 GDPR, l'interpretazione del concreto contenuto di questo dovere risulta strumentale per delineare i confini dell'eventuale inadempienza del DPO: è chiaro infatti che la responsabilità di quest'ultimo scema laddove non sia stato messo nella condizione di svolgere il proprio lavoro.

Se pensiamo al DPO esterno, perché questi possa diligentemente adempiere ai propri compiti è certamente necessario che il titolare gli offra un supporto concreto. Per esempio: organizzando i flussi di informazioni e dati necessari per l'espletamento delle sue funzioni, da parte delle funzioni aziendali coinvolte e da e per gli altri organismi di controllo, facendolo assistere alle riunioni ove

[24] V. art. 7 Stat. Lav. Si ricorda che per la corretta corrispondenza tra gravità della infrazione realizzata dal DPO e la sanzione applicabile si deve fare riferimento al contratto collettivo di riferimento.

[25] Sul punto v: Cass., Sez. lavoro, 26 giugno 2000, n. 8702 in *Mass. Giur. It.*, 2000; Cass., Sez. lavoro, 3 febbraio 1999, n. 950, in *Notiz. Giur. Lav.*, 1999; Cass., Sez. lavoro, 7 gennaio 1995, n. 208, in *Giur. It.*, 1996, I, 1, 687; Cass, Sez. lavoro, 5 aprile 1990, n. 2822, in *Mass. Giur. It.*, 1990; Cass., Sez. Lavoro, 29 novembre 1989, n. 5250, in *Mass. Giur. It.*, 1989.

vengono prese le decisioni rilevanti in materia di trattamento di dati personali e coinvolgendolo anche nei tavoli operativi in caso di nuovi progetti nonché garantendogli la possibilità di definire e attuare in autonomia programmi di verifica e controllo delle attività di trattamento dell'ente.

Il costante aggiornamento e il mantenimento di «*conoscenze specialistiche*» non pare invece che possa costituire un obbligo del titolare (o comunque solo del titolare) quando il DPO è esterno. Trattandosi di un professionista, è infatti ragionevole ritenere che l'onere di per sé ricada sullo stesso DPO, restando a carico del designante piuttosto un impegno formale a incentivare il DPO ad aggiornarsi e, quindi, al contempo a consentire ed agevolare la partecipazione del DPO a seminari, corsi e altre occasioni di formazione (ad esempio, indicando al DPO le tematiche in relazione alle quali è necessario un approfondimento poiché di particolare interesse per l'ente).

È naturalmente opportuno che il contratto di incarico del DPO contenga una declinazione pratica, per quanto esemplificativa, dell'obbligo in esame.

Inoltre, pare ragionevole che tra le pratiche utili a fornire al DPO il sostegno richiesto dalla legge debba essere annoverato anche il riconoscimento di un corrispettivo adeguato: un corrispettivo irrisorio, o comunque incoerente con la specialità della competenza e l'impegno richiesti, è sintomo di scarsa considerazione dell'importanza dell'attività del DPO per la propria organizzazione e dunque di un approccio puramente formale al tema.

Quanto al DPO interno, la questione presenta alcune peculiarità (soprattutto in relazione a quelle situazioni di soggetti già dipendenti della società che vengono poi destinati anche a tale incarico).

Non va dimenticato che ricade sul datore di lavoro quello che la dottrina definisce il *dovere di cooperazione* del datore all'adempimento del lavoratore, in applicazione del fondamentale principio di buona fede e correttezza contrattuale (art. 1175 c.c.), che comporta l'obbligo del datore di porre il dipendente nelle condizioni di potere assolvere correttamente al proprio incarico: ad esempio fornendogli gli strumenti idonei, carichi di lavoro proporzionali alle ore, etc.).

In relazione al DPO interno, rilevano quindi contestualmente a carico dell'ente: *(i)* in quanto datore di lavoro, gli obblighi "giuslavoristici" (di formare il proprio personale e di porre lo stesso nelle condizioni – anche organizzative – idonee a esercitare la propria mansione); *(ii)* in quanto designante del DPO, gli obblighi *ex* art. 38 GDPR (di fornire supporto adeguato al dipendente indicando espressamente i compiti attribuiti, le eventuali risorse assegnate per il loro svolgimento, nonché ogni informazione utile in rapporto al contesto di riferimento).

In altri termini, nel caso del DPO dipendente alcuni obblighi (come ad esempio quello formativo) a carico dell'ente/datore di lavoro presentano una duplice base legale, scaturendo in parallelo dal rapporto di lavoro subordinato e

dallo specifico ruolo di DPO che il dipendente ha assunto nell'organizzazione aziendale.

Nel caso poi del DPO interno già dipendente, e dunque già stabilmente inserito nell'organigramma aziendale, il datore di lavoro/designante dovrà prestare particolare attenzione nel rispettare il corretto inquadramento del lavoratore in relazione al contratto collettivo.

È possibile infatti che le ulteriori funzioni assegnate, gli aspetti di autonomia per legge attribuiti al DPO, le competenze professionali altamente specialistiche richieste assumano rilievo in relazione al livello di inquadramento del dipendente scelto, rendendo ad esempio necessario un "avanzamento" per adeguare le mansioni, le responsabilità, l'autonomia decisionale al livello spettante. Naturalmente, tali valutazioni rilevano anche nella individuazione della giusta retribuzione, dovendo il grado responsabilità affidata a un lavoratore costituire uno dei parametri rilevanti. Purtroppo, le prassi attualmente in voga si muovono nel senso opposto, con la conseguenza di attribuire importi irrisori rispetto alla funzione effettiva (potenzialmente non corretti a livello contrattuale) a un soggetto che, *ex lege* e nella sostanza, ricopre invece un ruolo di estrema rilevanza con riferimento alla regolarità dei trattamenti di dati personali aziendali.

6. Profili di responsabilità in caso di DPO in conflitto di interessi: inquadramento

L'altra circostanza in cui la nomina di un DPO può rivelarsi in contrasto con le prescrizioni normative, e dunque foriera di responsabilità, è quella del DPO in conflitto di interessi.

Si tratta di un tema di particolare attualità: la diffusa mancanza di consapevolezza e sensibilità in merito all'effettivo ruolo del DPO conduce nella pratica attuazione della normativa a frequenti fraintendimenti sul posizionamento del DPO nell'ambito dell'organizzazione aziendale dell'ente designante, sulle effettive funzioni di tale soggetto e sul ruolo dallo stesso assunto rispetto ai trattamenti di dati personali effettuati dell'ente e al relativo processo di adeguamento continuativo al GDPR.

Come visto, l'art. 38, par. 6, GDPR dispone che gli enti che lo designano devono «*assicurarsi*» che il DPO non agisca in conflitto di interessi, cioè non svolga funzioni/mansioni tali da dare adito a incompatibilità, trovandosi a controllare situazioni di gestione di dati personali da lui stesso determinate per posizione gerarchica o cui contribuisce o ha contribuito nella sua funzione aziendale o incarico professionale: quelle situazioni in cui, cioè, si trovi ad essere allo stesso tempo controllore e controllato.

Ciò posto, occorre domandarsi cosa succede se il DPO versa in conflitto di

interessi. In particolare, considerato che legge pone su chi nomina il DPO la responsabilità di assicurarsi che il conflitto non vi sia, il DPO in conflitto va esente da responsabilità?

Anche in questo caso le situazioni prospettabili cambiano a seconda che il DPO sia interno o esterno.

7. DPO interno in conflitto di interessi: azioni di prevenzione

Il DPO interno, nella maggior parte dei casi pratici, è un soggetto già dipendente dell'ente che continua a svolgere altre funzioni contestualmente a quella di DPO.

Come evitare in questo caso il conflitto?

Il GDPR omette di dettare specifiche misure per fare fronte al problema, che è coerentemente rimesso all'*accountability* del designante: è evidente che la chiave è una corretta gestione dell'assetto organizzativo aziendale, attività che spetta naturalmente al datore di lavoro (anche titolare o responsabile del trattamento).

Occorrerà quindi che il datore di lavoro, se sceglie il DPO tra soggetti già dipendenti dell'ente, svolga una rigorosa valutazione dell'organigramma della società evitando tra i candidati alla funzione di DPO – oltre a tutte le persone che non abbiano sufficiente esperienza e competenza – coloro che nell'esecuzione delle proprie mansioni lavorative abbiano, o abbiano avuto, influenza sulle decisioni relative al trattamento dei dati personali.

Chiaramente, il datore di lavoro dovrà anche avere cura di non affidare al dipendente DPO, successivamente alla nomina, altri incarichi che implichino la possibilità di assumere decisioni aziendali in materia di trattamento.

Al fine di evitare il concretizzarsi di tali situazioni, il gruppo di lavoro Articolo 29 Working Party (WP29, oggi European Data Protection Board – EDPB) (nelle Linee Guida WP243) e il Garante italiano (nelle FAQ) hanno stilato un elenco delle situazioni tipo in presenza delle quali è elevato il rischio di conflitto di interessi. Per quanto riguarda il settore pubblico si suggerisce ad esempio di evitare di nominare quale DPO, oltre a chi già è investito di ruoli manageriali di vertice, le figure apicali dell'amministrazione con capacità decisionali in ordine alle finalità e ai mezzi del trattamento, ivi compreso il responsabile IT (chiamato ad individuare le misure di sicurezza necessarie) e il responsabile dell'Ufficio di statistica; nel settore privato, si ritiene preferibile evitare di assegnare il ruolo di DPO a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale*, etc*.) ovvero funzioni aziendali aventi potere decisionale in ordine alle finalità e alle modalità/ai mezzi del trattamento (direzione risorse umane, direzione marketing, responsabile IT, etc.).

Anche l'European Data Protection Supervisor (EDPS), nel *Position Paper del 30.9.2018* ha esemplificato situazioni di incompatibilità rispetto all'assunzione del ruolo di DPO all'interno di un'organizzazione, sottolineando come l'esistenza del conflitto non si configuri necessariamente in rapporto a una situazione apicale [26].

Va inoltre considerato che il conflitto potrebbe instaurarsi sotto profili anche diversi dalla gestione dei dati personali: per esempio, nel caso di dipendente DPO "polifunzionale" può crearsi un conflitto legato al tempo assorbito dalle diverse funzioni assunte, che rischia di rendere inefficace l'azione del DPO [27]. In tale caso, possono e devono essere adottate prassi e azioni utili a perseguire un assetto organizzativo aziendale idoneo ad evitare l'instaurarsi del conflitto: per esempio, il datore di lavoro potrà indicare preventivamente il tempo destinato all'attività di DPO (compresa la formazione e l'aggiornamento) e quello da dedicare alle altre mansioni affidate.

8. Responsabilità dell'ente per il conflitto di interessi del DPO interno

Quanto alle conseguenze in capo all'ente designante, anche in caso di conflitto d'interessi del DPO esso è l'unico destinatario dell'obbligo di legale di *conformità* al GDPR dei trattamenti di dati personali ad esso riferibili, nel cui contesto si colloca il già richiamato obbligo di "assicurarsi" che il DPO non operi in conflitto di interessi.

Poiché tale risultato, nel caso del DPO interno, è strettamente connesso alle scelte organizzative del datore di lavoro, la responsabilità di un eventuale conflitto non può che essere imputabile esclusivamente al designante, il quale di conseguenza resta soggetto a una sanzione fino a € 10.000.000 o al 2% del fatturato annuo mondiale (ove superiore) [28]. Da un punto di vista pratico, spetterà dunque al datore di lavoro trovare la soluzione organizzativa idonea a prevenire

[26] https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf. V. par. 4.5: «Functions that would in principle be incompatible with the DPO function include high level positions within management, human resources, IT services, medical services, security services, internal audit, etc.» (…) «A conflict of interests may typically also arise (even for lower level positions), (…) when a DPO who is also part of the compliance team must assess compliance checks and related data processing that they have designed».

[27] V. in tale senso EDPS, Position Paper 30.9.2018, par. 4.3: «Experience has shown that part-time DPOs have found themselves in a permanent conflict between allocating time and efforts to their regular tasks as opposed to investing in their DPO duties».

[28] V. art. 83 par. 4 lett. a) GDPR.

o a fare cessare la situazione di incompatibilità (valutando eventualmente la revoca dell'incarico di DPO, ferme restando tutte le cautele di tipo giuslavoristico).

9. DPO esterno in conflitto di interessi: azioni di prevenzione

Passando al DPO esterno, incaricato tramite un contratto di servizi, innanzitutto si deve ricordare che le Linee Guida WP243 hanno precisato la possibilità di affidare tale incarico a un soggetto non persona fisica.

Come prevenire il rischio di conflitto di interessi, in questo caso?

Il WP29 ha indicato da un lato che i compiti del DPO «*potranno essere assolti efficacemente da un* team *operante* [però] *sotto l'autorità di un* [solo] *contatto principale designato*», quindi di una sola persona fisica che funga da «*"responsabile" per il singolo cliente*», per gli interessati e per il Garante; dall'altro lato, che «*è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale* DPO *soddisfi tutti i requisiti applicabili come fissati nel RGPD*» [29].

In ogni caso di nomina di un DPO è comunque consigliabile che il contratto di servizi sia sufficientemente preciso e dettagliato sul punto; ad esempio, è opportuno indicare le garanzie adottate per evitare che il DPO si trovi o venga successivamente a trovarsi in conflitto di interessi e inserire una dichiarazione espressa del DPO in merito all'assenza di incompatibilità (anche in relazione alla disponibilità di tempo o risorse da dedicare, pur in pendenza di altri incarichi per altri titolari), accompagnata dalla relativa garanzia e manleva.

È inoltre raccomandabile – in termini di documentazione di *accountability* e a fini di tutela del designante nei confronti del DPO stesso (*cfr. infra*) – attuare e documentare opportune verifiche.

Quanto al caso di DPO esterno di un ente pubblico, quindi nominato all'esito di un bando di gara, il tema è ancora più rilevante in quanto l'interesse dell'ente a selezionare soggetti dotati di specifici requisiti di affidabilità risponde a un interesse di portata generale.

---

[29] Nello stesso senso l'EDPS, cit., par. 4.4, con riferimento agli "assistant DPOS": «In practice, assistant DPOs not only assist the DPO, but also ensure the continuity of the function in the event of absence of the DPO. Despite the fact that the Regulation does not address the issue of the status of assistant DPOs, the EDPS believes that assistant DPOs should be offered the same guarantees as those provided for in the Regulation as concerns DPOs themselves. The same rules apply also to acting DPOs. The latter shall ensure in an independent manner the internal application of the Regulation, they may not receive any instructions in the performance of their duties, and their selection as acting DPO shall not be liable to result in a conflict of interests between his/her duty as acting DPO and any other official duties».

L'assenza di un conflitto di interessi in capo al candidato alla carica di DPO è un requisito necessario per lo svolgimento dell'incarico e quindi costituirà una condizione necessaria per la partecipazione alla gara. Il concorrente sarà dunque presumibilmente chiamato a dimostrare tale requisito o, quantomeno, a fornire una opportuna dichiarazione sostitutiva di notorietà, ai sensi dell'art. 47 del D.P.R. n. 445/2000, attestante l'assenza di conflitto di interesse.

10. Conseguenze del conflitto di interessi in termini di allocazione della responsabilità tra designante e DPO

Ciò chiarito, bisogna chiedersi cosa potrebbe succede qualora il DPO dovesse omettere di dichiarare l'esistenza di una situazione di conflitto, magari difficilmente conoscibile da parte del Titolare.

Quanto all'allocazione della responsabilità per le conseguenze dannose causate in capo al designante dal conflitto di interessi, valgono i principi generali che disciplinano i rapporti contrattuali: l'art. 1375 c.c. (in forza del quale «*Il contratto deve essere eseguito secondo buona fede*») e più in generale l'art. 1175 c.c. (correttezza del comportamento delle parti in tutti i rapporti obbligatori); e l'art. 1218 c.c. (in forza del quale «*Il debitore che non esegue esattamente la prestazione dovuta è tenuto al risarcimento del danno*»).

In sostanza, la buona fede – che si traduce in una serie di doveri di collaborazione, tra cui l'obbligo di informare di ogni questione che sia rilevante per la controparte – impone al DPO di comunicare l'eventuale incompatibilità al designante, pena la sua responsabilità nei confronti di quest'ultimo. Tuttavia, sotto il profilo risarcitorio assume rilievo anche l'art. 1227 c.c., in forza del quale «*se il fatto colposo del creditore ha concorso a cagionare il danno, il risarcimento è diminuito secondo la gravità della colpa e l'entità delle conseguenze che ne sono derivate. Il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza*».

Traducendo questi principî nel contesto in esame, il designante concorre con il DPO reticente quando non attua idonee verifiche preventive sulla effettiva assenza di conflitto.

Quindi, il designante non può limitarsi a farsi rilasciare dichiarazioni in tale senso da parte del DPO, ma per quanto possibile deve attivarsi per verificarle: ciò è perfettamente coerente con la già ricordata previsione dell'art. 38, par. 6 GDPR, che attribuisce al designante l'onere di "assicurare" che non vi sia conflitto di interessi.

Pertanto, in caso di concorso di colpa il designante non potrà vedersi riconosciuto il danno causato dalla reticenza del DPO oppure otterrà un risarcimento ridotto rispetto al pregiudizio subito; in mancanza di concorso, si deve invece

ritenere che la sussistenza di un conflitto d'interessi "occulto" possa integrare un inadempimento del DPO al contratto che lo lega al designante, con il conseguente riconoscimento del risarcimento del danno procurato a quest'ultimo.

Ciò appare particolarmente rilevante anche in considerazione del fatto che – come detto – l'ente resta comunque soggetto al rischio di sanzione fino a € 10.000.000 (o al 2% del fatturato annuo mondiale ove superiore) [30] nel caso in cui non provveda a nominare il DPO secondo le prescrizioni della legge, e pertanto anche nel caso in cui il DPO non sia indipendente o si riveli in conflitto di interessi.

11. Effetti del conflitto di interessi sul contratto di servizi tra privati

Un ultimo aspetto che è opportuno analizzare riguarda la sorte del contratto di servizi stipulato con il DPO in conflitto di interessi.

In linea generale, un tale accordo potrebbe essere: (a) risolto a fronte di un inadempimento del DPO alle garanzie assunte; (b) annullato, su richiesta del designante, ai sensi dell'art. 1439 c.c. [31]; (c) dichiarato nullo per contrarietà a norme imperative *ex* art. 1418 c.c., mancando in tale caso un requisito inderogabilmente previsto dalla legge [32].

12. Responsabilità del DPO in conflitto di interesse nominato attarverso gara pubblica

Quanto al DPO di un ente pubblico, poiché l'assenza del conflitto di interessi rappresenta un requisito necessario per lo svolgimento dell'incarico, il concor-

[30] V. art. 83, par. 4, lett. a) GDPR.

[31] Ai sensi dell'art. 1439 comma 1 c.c. «il *dolo* è causa di *annullamento* del contratto quando i raggiri usati da uno dei contraenti sono stati tali che, senza di essi, l'altra parte non avrebbe contrattato».

[32] A tale proposito si ritiene condivisibile l'orientamento giurisprudenziale secondo cui «in tema di nullità del contratto per contrarietà a norme imperative, l'area delle norme inderogabili di cui all'art. 1418, comma 1, c.c., ricomprende, oltre le norme relative al contenuto dell'atto, anche quelle che, in assoluto, oppure in presenza o in difetto di determinate condizioni oggettive e soggettive, direttamente o indirettamente, vietano la stipula stessa del contratto ponendo la sua esistenza in contrasto con la norma imperativa». Cfr. sul punto Cass., Sez. Lavoro, 21 aprile 2016, n. 8066, in *CED Cassazione*, 2016 che in applicazione del suddetto principio ha confermato la decisione di merito che aveva ritenuto la nullità di un accordo transattivo relativo al conferimento dell'incarico di direttore generale della RAI illecito perché stipulato in violazione dell'incompatibilità di cui all'art. 2, comma 9, legge n. 481/1995.

rente sarà presumibilmente chiamato a dimostrare tale requisito o quantomeno a fornire una dichiarazione sostitutiva di notorietà attestante l'assenza di conflitto. In base ai principi generali, l'eventuale falsa dichiarazione da parte del DPO rileverà ragionevolmente come causa di annullamento del provvedimento di assegnazione dell'incarico nonché come circostanza di per sé idonea e sufficiente a ledere irrimediabilmente il rapporto fiduciario tra concorrente e appaltante, con la conseguente responsabilità (anche risarcitoria) del candidato DPO nei confronti dell'ente. Peraltro, non si può escludere che una simile circostanza possa comportare anche la segnalazione all'ANAC.

THE GENERAL DATA PROTECTION REGULATION (GDPR) NELLA PUBBLICA AMMINISTRAZIONE

Valeria Manzo

Abstract:

The article, starting from the examination of the right of access (according to which all private subjects who have a direct, concrete and actual interest corresponding to a legally protected situation and connected to the document have the right to access the administrative documents), of the report between the protection of personal data and the principle of transparency (as an obligation for all Public Administrations to make their work visible and controllable externally in order to make administrative action available to third parties), aims to examine the General data protection regulation (EU) n. 2016/679 (better known as GDPR), as well as Legislative Decree no. 101 of 10 August 2018 laying down the provisions for the adaptation of the national legislation to the provisions of the aforementioned Regulation.

Key-words: GDPR – access right to administrative documents – treatment of sensitive data

Summary: 1. Il diritto di accesso e i dati sensibili. – 2. Protezione dei dati personali e trasparenza. – 3. Il trattamento dei dati sensibili nel GDPR. – 4. Il GDPR per la Pubblica Amministrazione.

1. Il diritto di accesso e i dati sensibili

L'accesso agli atti amministrativi (c.d. conoscitivo o informativo) è un diritto riconosciuto ai singoli cittadini in funzione dei rapporti con lo Stato e la Pubblica Amministrazione al fine di garantire la trasparenza di quest'ultima.

Secondo la tesi prevalente [1], la pretesa all'accesso, conformemente alla qua-

[1] *Ex multis* F. Bretoni, *Privacy e diritto d'accesso nella Pubblica Amministrazione*, Napoli, 2006, p. 34 ss.; F. Caringella, R. Garofoli, M.T. Sempreviva, *L'accesso a documenti amministrativi*, Milano, 2003, p. 56 ss.; A. Cauduro, *Il diritto di accesso a dati e documenti amministrativi*

lificazione normativa, ha natura di diritto soggettivo perfetto affidato alla giurisdizione esclusiva del G.A., chiamato a dirimere una controversia avente ad oggetto diritti in conflitto e non l'esercizio di un potere dell'amministrazione.

Tale qualificazione dell'accesso comporta che: 1) il decorso del termine per proporre il ricorso contro il diniego dell'accesso non impedisce all'interessato di far valere il diritto di accesso nell'ordinario termine di prescrizione; 2) nel corso del giudizio dinanzi al GA deve ammettersi la possibilità della PA di addurre nuove ragioni che giustificano il diniego dell'accesso e 3) la mancata notificazione del ricorso ad almeno uno dei controinteressati non rende inammissibile in ricorso stesso, ma obbliga il giudice ad integrare il contraddittorio per assicurare la partecipazione dei litisconsorti a norma dell'art. 102 c.p.c.

Il Capo V della Legge n. 241/1990 sul procedimento amministrativo disciplina l'accesso ai documenti amministrativi.

Titolari del diritto sono, ai sensi dell'art. 22, lett. b) della summenzionata Legge, tutti i soggetti c.d. interessati (privati ovvero portatori d'interessi diffusi) i quali abbiano un interesse corrispondente ad una situazione giuridica tutelata e connessa al documento in relazione al quale si richiede l'accesso.

In particolare, l'interesse dev'essere: attuale (non avuto riguardo all'interesse ad agire in giudizio per la tutela della posizione sostanziale vantata, bensì alla richiesta di accesso ai documenti); diretto (ovvero appartenente alla sfera dell'interessato (e non ad altri soggetti) e concreto (con riferimento alla necessità di un collegamento tra il soggetto ed un bene della vita coinvolto dall'atto o documento).

Secondo la dottrina prevalente l'interesse deve, inoltre, essere: serio (meritevole e non emulativo); adeguatamente motivato, con riferimento alle ragioni che vanno esposte nella domanda di accesso e deve corrispondere ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso [2].

Oggetto del diritto d'accesso sono i documenti amministrativi definiti dalla lett. d) dell'art. 22 come novellato dalla Legge n. 15/2005 come "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni o, comunque utilizzati ai fini dell'attività amministrativa*".

La norma ha risolto in maniera positiva il problema se oggetto del diritto di

---

come promozione della partecipazione: un'innovazione limitata, in *Diritto Amministrativo*, 3/2017, Milano, pp. 601-623; A. Romano Tassone, *A chi serve il diritto di accesso? (riflessioni su legittimazioni e modalità di esercizio del diritto di accesso nella L. n. 241 del 1990)*, in *Dir. amm.*, 1995, p. 315 ss.; G. Tulumello, *Brevi note sull'attuale disciplina dell'accesso agli atti amministrativi*, in *Giur. mer.*, 2007, p. 6 ss.

[2] S. Cimini, *Accesso ai documenti amministrativi e riservatezza: il legislatore alla ricerca di nuovi equilibri*, in *Giustizia civile*, 2005, 10, p. 407 ss.

accesso possano essere anche gli atti interni, ovvero gli atti endoprocedimentali costituenti gli antecedenti del provvedimento finale (si pensi ai pareri tecnici ed al nulla osta) e se tale diritto possa riguardare anche gli atti di diritto privato emessi dalla P.A.

Il nuovo testo dell'art. 23 definisce l'ambito dei soggetti nei cui confronti è esercitabile il diritto di accesso ai documenti ovvero: di tutte le pubbliche amministrazioni (non più solo statali); delle aziende autonome e speciali e degli enti pubblici e dei gestori di pubblici servizi.

L'art. 24 della Legge *de qua*, è stato fortemente innovato dalla Legge n. 15/2005 la quale ha previsto vari livelli di limitazioni al diritto di accesso.

L'accesso è escluso: 1) per tutti i documenti coperti dal segreto di Stato ai sensi delle vigenti disposizioni di legge e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge o dal regolamento governativo di attuazione; 2) nei procedimenti tributari, per i quali restano ferme le particolari norme regolatrici; 3) nei confronti delle attività della P.A. dirette all'emanazione di atti normativi, atti amministrativi generali, di programmazione e pianificazione e 4) nei procedimenti selettivi, quando vengono in rilievo documenti contenenti informazioni di natura psico-attitudinale relativi a terzi.

Fuori da queste ipotesi, il nuovo sesto comma dell'articolo in esame enuncia la regola di principio secondo cui il diritto di accesso può essere escluso per l'esigenza di salvaguardare: la sicurezza, la difesa nazionale e le relazioni internazionali; la politica monetaria e valutaria; l'ordine pubblico e la prevenzione e repressione della criminalità; la vita privata o la riservatezza di persone fisiche, giuridiche, gruppi, imprese ed associazioni con particolare riferimento agli interessi di natura epistolare, sanitaria, finanziaria, industriale e commerciale, nonché l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

Le modalità di esercizio del diritto di accesso sono disciplinate dall'art. 25, commi primo-quarto della Legge n. 241/1990 e dagli artt. 3-7 del D.P.R. n. 352/1992.

L'interessato, al fine di esaminare ovvero estrarre copia di documenti, deve formulare una motivata richiesta (formale o informale), presentata all'ufficio dell'amministrazione competente a formare l'atto conclusivo del procedimento o a detenere stabilmente il relativo documento.

È discusso se sia applicabile l'art. 7 della Legge n. 241/1990 che impone di dare comunicazione dell'avvio del procedimento; appare, tuttavia, preferibile aderire all'orientamento negativo secondo il quale, privilegiando la legge il rapido svolgimento della procedura di accesso, tale finalità appare incompatibile con l'obbligo di dare avviso dell'inizio del procedimento [3].

[3] F. Ferrara, *Diritto di acceso ai documenti ammnistrativi ed il limite del controllo generaliz-*

Entro trenta giorni dalla richiesta, la P.A. deve esprimere le sue determinazioni.

Nel caso in cui accolga la richiesta, indica le modalità e fissa il termine (non inferiore a quindici giorni) per prendere visione dei documenti o ottenerne copia. Sul punto, attenziona come il diritto all'accesso possa anche essere realizzato mediante la pubblicazione degli atti nella Gazzetta Ufficiale o secondo le modalità previste dai singoli ordinamenti, comprese le forme di pubblicità attuabili mediante strumenti informatici, elettronici e telematici.

Diversamente, qualora rifiuti l'accesso, totalmente o parzialmente, ovvero lo differisce, il responsabile del procedimento, ai sensi del terzo comma dell'art. 25 della Legge n. 241/1990, deve motivare il provvedimento con riferimento specifico alla normativa vigente, alle categorie di atti per i quali è stato escluso l'accesso dai regolamenti delle singole amministrazioni e alle circostanze di fatto che rendono non accoglibile la richiesta così come proposta [4].

2. Protezione dei dati personali e trasparenza

La trasparenza, quale chiarezza e comprensibilità dell'azione amministrativa, è un valore-chiave dell'ordinamento democratico espressamente incluso, dall'art. 1 della Legge n. 241/1990, tra i principi generali che regolano l'attività amministrativa capace di coniugare l'efficienza nello svolgimento della funzione pubblica con le garanzie di tutela delle posizioni giuridiche degli amministrati [5].

Suoi inscindibili corollari sono gli obblighi di pubblicità (che si sostanziano nel diritto d'informazione cui l'amministrazione è tenuta a beneficio indiscriminato di tutti i consociati) ed il diritto di accesso, quali strumenti approntati dall'ordinamento per garantire la trasparenza e realizzarla in concreto [6].

Il comma 1 dell'art. 1 della Legge 7 agosto 1990, n. 241, come riscritto dalla Legge 11 febbraio 2005, n. 15, introduce il principio di trasparenza come regola di condotta della pubblica amministrazione.

La necessità di un controllo democratico da parte dei cittadini sull'operato

---

zato sull'operato della pubblica amministrazione: il caso dei risultati scolastici, in *Foro amm.*, CDS, I, 2011, p. 300 ss.

[4] M. Lasalvia, *Il diritto di accesso ai documenti delle Pubbliche Amministrazioni*, Roma, 2006, p. 210 ss.

[5] G. Arena, *Trasparenza amministrativa*, in S. Cassese, *Dizionario di diritto pubblico*, Milano, 2006, p. 5945 ss.

[6] A. Sandulli, *Il procedimento amministrativo e la trasparenza*, in S. Cassese, C. Franchini (a cura di), *L'amministrazione pubblica italiana*, Bologna, 1994, p. 101 ss.

della P.A. impone che l'attività di questa sia sottoposta a pubblicità con conseguente obbligo di pubblicazione, comunicazione e accessibilità di notizie, documenti, atti e procedure [7].

Tale criterio porta l'Amministrazione a rendere visibile e controllabile all'esterno il proprio operato affinché sia conforme agli interessi sociali ed ai principi costituzionali.

Sulla scia dei nuovi istituti introdotti prima dal d.lgs. n. 150/2009 e, successivamente, dal d.lgs. n. 33/2013 (noto come "Decreto trasparenza") si è operata un'importante estensione dei confini della trasparenza, intesa oggi come testualmente recita l'art. 1, primo comma, del d.lgs. n. 33/2013 come "*accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*".

In questo rinnovato contesto, l'ampio diritto all'informazione ed alla trasparenza dell'attività delle amministrazioni resta temperato solo dalla necessità di garantire le esigenze di riservatezza, segretezza e tutela di determinati interessi pubblici e privati (come elencati nell'art. 5-*bis* del d.lgs. n. 33/2013) che diventano l'eccezione alla regola della libertà d'informazione [8].

Le linee guida emanate dal Garante Privacy alla luce del d.lgs. in esame riguardano sia la pubblicazione di dati e documenti che le Pubbliche Amministrazioni devono inserire *on line* per finalità di trasparenza, sia di quelli finalizzati a garantire altri obblighi di pubblicità degli atti amministrativi (si pensi alle pubblicazioni matrimoniali ovvero all'avviso di deposito delle cartelle esattoriali).

Tali le principali misure indicate per la trasparenza *on line*:

– le P.A. devono pubblicare solo dati esatti, aggiornati e contestualizzati;

– prima di inserire *on line* sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali, le amministrazioni devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo;

– le Pubbliche Amministrazioni devono pubblicare *on line* solo dati la cui pubblicazione risulti realmente necessaria (se deve ritenersi sempre vietata la pubblicazione di dati sulla salute e sulla vita sessuale, i dati sensibili quali etnia, religione ed appartenenze politiche possono essere diffusi solo laddove indispensabili al perseguimento delle finalità di rilevante interesse pubblico);

– occorre adottare misure per impedire l'indicizzazione dei dati sensibili da parte dei motori di ricerca e il loro riutilizzo;

---

[7] S. Foà, *La nuova trasparenza amministrativa*, in *Diritto Amministrativo*, 1/2017, Milano, pp. 65-100.

[8] M. Savino, *La nuova disciplina ella trasparenza amministrativa*, in *G.d.A.*, 2013, p. 8 ss.

– qualora le P.A. intendano pubblicare dati personali ulteriori rispetto a quelli individuati nel "Decreto trasparenza", dovranno procedere prima all'anonimizzazione di essi;

– l'obbligo previsto dalla normativa in materia di trasparenza *on line* della P.A. di pubblicare dati in "formato aperto", non comporta che questi siano anche "dati aperti" ovvero liberamente utilizzabili da chiunque per qualunque scopo (il riutilizzo dei dati personali non dovrà, in alcun caso, pregiudicare, anche sulla scorta della direttiva europea in materia, il diritto alla privacy);

– le Pubbliche Amministrazioni dovranno inserire nella sezione denominata "Amministrazione trasparente" sui propri siti *web* un *alert* con cui si informa il pubblico che i dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto del norme sulla protezione dei dati personali;

– il periodo di mantenimento *on line* dei dati è stato generalmente fissato in 5 anni dal Decreto in esame (sono, tuttavia, previste alcune deroghe, come nell'ipotesi in cui gli atti producano i loro effetti oltre questa scadenza);

– l'obbligo d'indicizzare i dati nei motori di ricerca generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza (vanno, pertanto, esclusi i dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (si pensi alla pubblicità legale sull'albo pretorio);

– non possono, in alcun caso, essere indicizzati i dati sensibili e giudiziari [9].

3. Il trattamento dei dati sensibili nel GDPR

Il Parlamento Europeo ed il Consiglio, considerando che: 1) la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale come sancito dagli articoli 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea; 2) i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettarne i diritti e le libertà fondamentali e, in particolare, il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza; 3) la rapidità dell'evoluzione tecnologica e la globalizzazione comporta che le persone fisiche abbiano il controllo dei dati personali che li riguardano e godano di un rafforzamento della certezza giuridica e operativa; 4) la necessità di assicurare

[9] B. Ponti, *Nuova trasparenza amministrativa e libertà di accesso alle informazioni. Commento sistematico al D.Lgs. 33/2013 dopo le modifiche apportate dal D.Lgs. 25 maggio 2016, n. 97*, Sant'Arcangelo di Romagna, 2016, p. 98 ss.

un elevato livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei propri dati, hanno adottato il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (c.d. Regolamento generale sulla protezione dei dati – GDPR) [10].

Il Regolamento, definendo i dati personali alla stregua di qualsivoglia informazione riguardante una persona fisica identificata o identificabile (c.d. interessato), sancisce che essi debbano essere: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. principio di minimizzazione dei dati); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (c.d. principio di esattezza); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (c.d. pr. della limitazione della conservazione) e f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (c.d. principio d'integrità e riservatezza) [11].

L'innovazione più significativa del Regolamento è rappresentata dalla previsione dell'RPD (responsabile per la protezione dei dati) quale persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratti dati personali per conto del titolare del trattamento che elabora i dati personali per conto del titolare del trattamento.

Il responsabile, nello specifico, è tenuto:

– a rispettare gli obblighi di trasparenza (in tal senso occorre contrattualizzare il rapporto tra titolare e responsabile, specificando gli obblighi e i limiti del

[10] L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 122 ss.

[11] S. Cassese, *Diritto amministrativo comunitario e diritti amministrativi nazionali*, in *Trattato di diritto amministrativo europeo*, Milano, 1997, p. 9 ss.

trattamento dati. Il responsabile riceverà tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi, dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'art. 28 del Regolamento e, da ultimo, dovrà tenere il registro dei trattamenti svolti);

– a garantire:

– la sicurezza dei dati (adottando tutte le misure di sicurezza adeguate al rischio tra le quali anche le misure di attuazione dei principi di *privacy by design* e *by default*);

– la riservatezza dei dati;

– ad avvisare (qualora ritenga che un'istruzione ricevuta violi qualche norma in materia), assistere (nella conduzione di una valutazione di impatto) e fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile.

Tali sono i diritti che l'interessato può ottenere dal titolare del trattamento:

– ai sensi dell'art. 15 GDPR la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine e h) l'esistenza di un processo decisionale automatizzato;

– ai sensi dell'art. 16 GDPR la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo;

– ai sensi dell'art. 17 GDPR la cancellazione (c.d. diritto all'oblio) dei dati personali che lo riguardano senza ingiustificato ritardo;

– ai sensi dell'art. 18 GDPR la limitazione del trattamento allorquando ricorra una delle seguenti ipotesi: a) l'interessato contesti l'esattezza dei dati personali; b) il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si sia opposto al trattamento in attesa

della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato;

– ai sensi dell'art. 20 GDPR ricevere in un formato strutturato i dati personali che lo riguardano forniti a un titolare del trattamento, nonché trasmettere tali dati ad un altro titolare del trattamento [12].

Nel caso in cui un tipo di trattamento possa presentare un elevato rischio per i diritti e le libertà delle persone fisiche, allorché preveda l'uso di nuove tecnologie, il titolare del trattamento dovrà preventivamente effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali – c.d. PIA (*Privacy Impact Assessment*).

Tale valutazione sistematica e globale di aspetti personali relativi a persone fisiche (basata su un trattamento automatizzato, compresa la profilazione) dovrà contenere una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; una valutazione della necessità e della proporzionalità dei trattamenti in relazione alle finalità, nonché una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontarli.

4. Il GDPR per la Pubblica Amministrazione

Seppur il Regolamento UE sia entrato in vigore il 24 maggio 2016, esso ha trovato applicazione negli Stati solo dal 25 maggio 2018.

Da tale data, dunque, le P.A. hanno iniziato ad applicare il regolamento e sono diventate cogenti le responsabilità e le sanzioni previste dal GDPR.

È, così, divenuto prioritario per ciascuna amministrazione definire internamente quale sia l'ufficio che si occupi stabilmente dell'adeguamento al GDPR e, in generale, degli adempimenti da questo previsti (dalla revisione delle informative alla istituzione e tenuta del registro delle attività di trattamento) [13].

Per semplificare l'applicazione del Regolamento, il nostro legislatore ha deciso di non abrogare il d.lgs. n. 196/2003 (rubricato Codice in materia di protezione dei dati personali), bensì di armonizzarlo con i contenuti del GDPR, prevedendone, così, un'abrogazione parziale.

Dal 19 settembre 2018, data di entrata in vigore del d.lgs. 10 agosto 2018, n. 101 (rubricato Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e

[12] P. Voigt, A. Von Dem Bussche, *The EU general data protection regulation (GDPR). A practical guide*, Cham, Springer, 2017, p. 45 ss.

[13] S. Comellini, *Il Regolamento Generale sulla Protezione dei dati personali e la nomina del DPO nella Pubblica Amministrazione*, Santarcangelo di Romagna, 2018, p. 32 ss.

del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (rubricato Regolamento generale sulla protezione dei dati), l'intera normativa italiana in materia di protezione dati dev'essere interpretata ed applicata alla luce del dettato del GDPR.

Tali le principali novità introdotte dal Decreto Legislativo *de quo*:

– per quanto riguarda il regime sanzionatorio, in ossequio al principio penalistico del *favor rei*, il decreto in esame sostituisce le sanzioni penali previste dal Codice privacy con le sanzioni amministrative previste dal Regolamento europeo anche avuto riguardo a violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso e sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili;

– vengono, inoltre, inseriti stante la crescente preoccupazione per i *cyber* attacchi a strutture critiche (quali, tra gli altri, gli ospedali) che trattano grandi quantità di dati personali, gli artt. 167-*bis* (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala) e 167-*ter* (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).

Cinque sono le fasi che le Pubbliche Amministrazioni dovranno seguire:

1) *privacy assessment* (che presuppone una mappatura dei ruoli e dei trattamenti in conformità alle disposizioni incluse nel GDPR. Devono essere rilevate le informazioni che riguardano le categorie dei dati trattati, le finalità del trattamento, le misure di sicurezza previste per la protezione dei dati, i destinatari delle comunicazioni dei dati e le categorie dei soggetti interessati);

2) definizione del modello organizzativo *privacy* in funzione delle informazioni che sono state ottenute in precedenza (è necessario identificare le figure della Pubblica Amministrazione che sono coinvolte nel trattamento dei dati, dai responsabili ai titolari, per attribuire loro le responsabilità e i ruoli relativi. Si disegnano, così, i c.d. dei processi di PIA – *privacy impact assessment*, di *privacy by design*, *privacy by default* e di notifica dei *data breach*);

3) *implementation and data protection management* (si predispongono: i servizi per le attività dei responsabili del trattamento, per la gestione delle procedure di data protection e la loro manutenzione e per la definizione dei piani di trattamento del rischio, nonché i servizi per l'esecuzione del *privacy impact assessment*, dell'*audit privacy* e per l'attività del DPO);

4) una volta che i flussi di dati sono stati mappati, che la struttura organizzativa per la protezione dei dati è stata definita e che i processi sono stati identificati, si gestisce il sistema di protezione in via continuativa della P.A. con revisione periodica delle procedure e dei processi privacy;

5) attivazione del processo di *audit privacy della P.A.* (verifica degli adempimenti imposti dal GDPR per accertarsi che siano state adottate tutte le misure organizzative e tecniche previste nel rispetto del principio di *accountability* dei responsabili e del titolare) [14].

In conclusione, trascorso quasi un anno dalla piena applicazione del GDPR, risultando ancora basso il livello di consapevolezza della protezione dei dati, in un'ottica di piena *governance* dei dati stessi, resta l'interrogativo: a che punto sono le Pubbliche Amministrazioni?

[14] A. Ciccia Messina, *La privacy nella pubblica amministrazione. Cosa cambia dopo il GDPR e il D.Lgs. n. 101/2018*, Federprivacy, 2019, p. 98 ss.

AI e GDPR:
L'AUTOMATED DECISION MAKING, LA PROTEZIONE DEI DATI E IL DIRITTO ALLA 'INTELLEGIBILITÀ' DELL'ALGORITMO

Emiliano Troisi

Key-words: AI – automated decision-making – data protection – algorithm disclosure

Category: Legal Area

Topic: Data Protection Law

Summary: 1. Introduzione. – 2. ADM: il divieto generale di trattamenti decisionali automatizzati, eccezioni e condizioni. (*Segue*). La speciale protezione dei minori d'età. – 3. Art. 22 del Regolamento: una fattispecie ampia. – 4. Una disciplina 'comune' dei trattamenti automatizzati. – 5. Il diritto alla 'intelligibilità' dell'algoritmo: un'interpretazione sistematica e coerente del GDPR. – 6. L'Accountability, l'obbligo di DPIA e il ruolo della privacy by design e by default nel futuro di una data-driven society. – 7. Impressioni conclusive.

1. Introduzione

Il Regolamento Generale sulla Protezione dei dati, il Reg. 2016/679/UE, in sigla GDPR, nasce e muove i suoi primi passi in una società digitale e in rapida e continua evoluzione. Tra IoT, Big Data Analytics, machine learning e Intelligenza Artificiale in tutte le sue applicazioni, ogni persona fisica, in ogni momento, è interessata da un trattamento dei propri dati o vi è potenzialmente soggetta. Sistemi di Profilazione e Data Analysis scovano correlazioni tra questi dati, e da questi estrapolano altri dati; predicono comportamenti, carpiscono interessi, intuiscono debolezze. Gli interessati e i loro dati, da oggetto del trattamento ne diventano spesso il 'prodotto'. Sulla base di questo 'prodotto' altri sistemi di IA decidono; a volte sbagliano, e quando sbagliano non è più soltanto la privacy del data-subject ad essere in pericolo ma il suo diritto a non essere

discriminato, ad avere un libero ed equo accesso a beni e servizi, a non essere manipolato a sua insaputa da forme di marketing scorrette, aggressive e invadenti, ma anche la legittima pretesa a contestare le decisioni lesive di una macchina o, soprattutto, a che queste non siano assunte in modo poco trasparente e sulla base, magari, di dati errati e incompleti.

A tutto questo il nuovo Regolamento Privacy risponde con una tutela più ampia e decisa rispetto al passato, una tutela che si estende oltre la mera protezione dei dati e fino a ricomprendere ogni diritto e libertà dell'individuo che possa esserne minacciata; diversa anche la prospettiva: destinatario delle norme è non più chi sia soggetto ad un trattamento del dato ma ogni persona fisica che vi possa essere potenzialmente coinvolta. Ancora, il GDPR introduce i concetti di rischio e accountability: in una società caratterizzata dalla circolazione continua e dinamica dei dati, in cui le modalità del trattamento come pure le sue finalità cambiano continuamente e diventano più complesse, anche la tutela degli interessati, per essere efficace, deve essere dinamica e parametrata, caso per caso, alle specifiche criticità.

Il presente articolo si soffermerà sulla pratica dei trattamenti decisionali automatizzati, o Automated Decision-Making, trattamenti condotti esclusivamente mediante applicazioni di Intelligenza Artificiale e potenzialmente anche molto lesivi della sfera giuridica soggettiva di chi vi sia sottoposto. Se ne individuerà la disciplina prevista nella cornice del GDPR, a partire dalle ridotte ipotesi in cui sono consentiti, i diritti e le specifiche cautele contemplate dal Regolamento, proponendo un'interpretazione ampia e di sistema dell'art. 22 e delle norme ad esso collegate.

Si indugerà, in particolare, sugli specifici e pregnanti oneri informativi posti a carico del titolare del trattamento, tentando di dimostrare come si spingano fino a richiedere una vera e propria '*disclosure*' degli algoritmi decisionali, a beneficio della consapevolezza degli interessati ma anche funzionale ad assolvere specifici obblighi di accountability.

In conclusione un accenno al ruolo sempre più centrale, e di peculiare importanza, che assumono e vanno sempre più assumendo, in questo ambito, la privacy by design e by default.

2. ADM: il divieto generale di trattamenti decisionali automatizzati, eccezioni e condizioni

Come anticipato, il GDPR raccoglie la sfida dell'Intelligenza Artificiale applicata al trattamento dei dati personali rispondendone a tutti i potenziali rischi con la previsione di una disciplina a tutela dei soggetti coinvolti che risulta par-

ticolarmente forte, incardinata su di uno stringente divieto generale di trattamento automatizzato senza consenso e ulteriormente arricchita di speciali misure e oneri informativi a carico del titolare del trattamento – come si vedrà, particolarmente gravosi – e diretti ad assicurare all' interessato il più ampio potere di controllo possibile sull'utilizzo dei propri dati.

L'art. 22 del Regolamento, infatti, espressamente sancisce il diritto dell'interessato a "non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Il riferimento è al cosiddetto Automated Decision Making (o più brevemente ADM), ovvero quel fenomeno per cui un sistema informatico programmato per assolvere a una specifica funzione o erogare un certo servizio della società dell'informazione è in grado di assumere, grazie ad un meccanismo inferenziale algoritmizzato – e perciò senza coinvolgimento umano –, una decisione rilevante per i soggetti interessati dalla stessa e basandosi a tal fine unicamente su una valutazione automatizzata dei loro dati personali o una profilazione degli utenti.

Il divieto di ADM, ai sensi del paragrafo 2 dello stesso articolo, non si applica solo se, e nella misura in cui i trattamenti decisionali automatizzati sono necessari per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento oppure siano basati sul consenso dell'interessato.

La possibilità di ricorrere lecitamente a trattamenti di questo tipo è quindi estremamente ristretta: non tutte le circostanze normalmente ammesse dall'art. 6 (1) (a-f) del Regolamento quali base giuridica del trattamento valgono a legittimare il trattamento condotto con meccanismi informatici automatizzati. L'ADM è ammesso solo in presenza di quelle condizioni autorizzative per così dire "consensuali", idonee ad assicurare una più ampia consapevolezza dell'interessato, con la conseguenza che deve ritenersi illegittimo in tutti i casi in cui l'interessato non vi abbia acconsentito espressamente attraverso una propria consapevole manifestazione di volontà, o direttamente [1], o nell'ambito di un più complesso rapporto contrattuale, sul presupposto però, in quest'ultimo caso, che il trattamento automatizzato sia da considerarsi necessario [2] alla conclusione o all'esecuzione dell'accordo.

---

[1] E per una o più finalità specificamente individuate, ai sensi dell'art. 6 (1) (a) GDPR.

[2] Il paragrafo 2, lett. a) dell'art. 22 GDPR contenente un'esenzione dal generale divieto di ADM deve essere interpretato, in ragione del suo carattere derogatorio, in senso restrittivo e pertanto perché il trattamento decisionale automatizzato possa essere considerato legittimo questo deve risultare, considerate le circostanze del caso, l'unico strumento possibile ovvero l'unico praticamente utilizzabile per raggiungere lo scopo contrattuale. In tal senso anche le *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251, p.23,* adottate dal Gruppo dell'articolo 29 per la tutela dei dati il 3 ottobre 2017.

In entrambe queste ipotesi in cui il trattamento decisionale automatizzato sia consentito, il titolare del trattamento ha, inoltre, il dovere - ai sensi del paragrafo 3 dell'esaminando art. 22 GDPR - di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi del *data subject*, e tra questi, in particolare, è tenuto in ogni caso a garantirgli il diritto ad ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestarne la decisione.

Ciò detto, bisogna aggiungere che il GDPR ammette pure che possa essere consentito – ai sensi del paragrafo 2, lett. b) dell'articolo in esame - adottare decisioni sulla base di un trattamento automatizzato in altre singole ipotesi previste da apposita norma autorizzativa del diritto dell'Unione o dello Stato Membro cui è soggetto il titolare del trattamento; ciò eccezionalmente pur in assenza del consenso dell'interessato e sempre che siano, anche qui, adottate misure adeguate alla tutela delle persone fisiche coinvolte. Secondo il Considerando 71 del Regolamento queste ipotesi possono includere, ad esempio, l'utilizzo di trattamenti informatizzati a fini di monitoraggio o prevenzione di frodi od evasione fiscale, ma in ogni caso deve ritenersi necessario – a parere di chi scrive – che il ricorso a tali meccanismi risulti giustificato alla luce del perseguimento di scopi di rilevante interesse pubblico e la relativa compressione dei diritti e delle libertà dei soggetti coinvolti sia proporzionata. In questi casi il Regolamento si limita a prescrivere l'obbligo per il legislatore di prevedere misure adeguate a tutela dei singoli ma il diritto a richiedere l'intervento umano e a contestare eventualmente la decisione non risulta assicurato dal paragrafo 3 dell'art. 22 (come invece negli altri casi esaminati), seppur nulla toglie, ovviamente, che le norme autorizzative di tali trattamenti, nel prevedere le salvaguardie richieste, possano predisporre forme di tutela anche più ampie.

Va infine sottolineato che sono in ogni caso vietati i trattamenti automatizzati e le profilazioni che coinvolgano i dati sensibili di cui all'art. 9 del GDPR, salvo che l'interessato abbia prestato il proprio consenso esplicito o questo sia consentito da apposita base normativa nel diritto dell'Unione o degli Stati Membri e purché il trattamento sia necessario per motivi di interesse pubblico e proporzionato alla finalità perseguita.

(*Segue*). La speciale protezione dei minori d'età

Un ulteriore appunto può farsi in merito ai trattamenti che riguardino minori d'età. L'art. 22 di per se non introduce obblighi diversi né tratta in maniera distinta l'ipotesi in cui l'ADM interessi minori d'età. Sebbene il dettato del Considerando 71, per quanto laconicamente, restituisca una chiara volontà, nelle in-

tenzioni del legislatore europeo, di negare l'ammissibilità di decisioni basate unicamente su trattamenti automatizzato che producano effetti giuridici o comunque incidano significativamente su minori ("Tale misura non dovrebbe riguardare un minore"), tale assunto non è raccolto dalla disposizione regolamentare approvata, con la conseguenza che trattamenti decisionali automatizzati che riguardino minori devono ritenersi leciti nelle medesime ipotesi in cui l'ADM sia consentito per gli adulti a norma del citato paragrafo 2 dell'art. 22 del Regolamento.

La norma tuttavia va contestualizzata e letta nell'ambito delle particolari tutele che in ogni caso, in via generale, il GDPR accorda ai minori che siano interessati da un trattamento dei dati. Il bisogno di una particolare protezione dei minori emerge innanzitutto chiaramente dal Considerando 38 che attesta la necessità di specifiche misure di salvaguardia, specialmente nel caso di raccolta di dati all'atto di servizi informatici offerti direttamente al minore per scopi di profilazione e marketing, in ragione proprio della minor consapevolezza dei rischi e delle conseguenze del trattamento dei propri dati che ci si possa ragionevolmente aspettare da loro per via della tenera età.

In ragione di ciò deve ritenersi quindi fuori di dubbio che il titolare del trattamento debba farsi carico, in caso di trattamenti automatizzati *ex* art. 22, di oneri specifici: ad esempio le misure adeguate a tutela dei diritti e delle libertà dell'interessato richieste dal paragrafo 3 dovranno certamente essere parametrate, in caso di minori, alla speciale protezione evocata nella cornice delle norme europee sulla privacy. Altrettanto pacificamente, nelle ipotesi in cui i trattamenti automatizzati poggino su base consensuale (verosimilmente la stragrande maggioranza dei casi) deve pure farsi applicazione della particolare disciplina di cui all'art. 8 GDPR; questa pone particolari condizioni al consenso al trattamento prestato dai minori, oltre che peculiari oneri di salvaguardia a carico del titolare del trattamento a cagione della speciale vulnerabilità che caratterizza la categoria di interessati in questione. Ove il trattamento di cui all'art. 22, paragrafo 2 si giustifichi in quanto necessario alla conclusione od esecuzione di un contratto tra il minore e il responsabile del trattamento, trovano poi applicazione anche tutte le norme di diritto interno relative alla validità ed efficacia di contratti conclusi dal minore di età [3].

3. Art. 22 del Regolamento: una fattispecie ampia

Orbene, individuati i casi in cui è consentita, a norma del GDPR, l'Automated

[3] Cfr. sul tema, Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017.

Decision Making e una prima parte della sua disciplina, prima di passare all'esame della rimanente parte delle norme che applicabili - che, come accennato, impongono al titolare del trattamento di predisporre talune salvaguardie tra cui almeno il diritto all'intervento umano, ma anche, per quanto in questa sede maggiormente interessa, del tutto peculiari oneri di trasparenza e informazione che si estendono alla 'logica' dell'algoritmo - è opportuno soffermarsi sulla fattispecie di cui all'art. 22 (1) del Regolamento ed individuare cosa si intenda per (e quindi in quali casi trovi applicazione la disciplina in esame) "decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che [...] riguardano direttamente [l'interessato, ndr] o che incida in modo analogo significativamente sulla sua persona.

Di trattamento automatizzato il Regolamento non dà una precisa definizione, l'art. 22 (1) vi include però espressamente la profilazione. Ai sensi dell'art. 4, per profilazione, nell'ambito del GDPR, si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di questi per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare e prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica". La profilazione è quindi una specie di trattamento automatizzato che consiste nell'esercizio, da parte di un software, un motore inferenziale, di un'operazione deduttiva capace di ricavare cioè da una certa quantità di dati inseriti in un data-set – analizzati e individuate tra loro, automaticamente, delle correlazioni statistiche – altri dati relativi a caratteristiche o schemi comportamentali attribuibili ad un determinato individuo o gruppi di essi al fine di classificarlo/i in precisi gruppi o categorie e/o predirne probabili comportamenti futuri.

Categoria più ampia della profilazione, dunque, per trattamento automatizzato deve intendersi in generale ogni raccolta e analisi di dati personali compiuta automaticamente da un agente informatico programmato a tale scopo.

I trattamenti automatizzati di cui all'art. 22 GDPR rilevano inoltre, espressamente, solo in quanto siano 'decisionali', conducano cioè ad (e applichino) una decisione che influisca sull'interessato. Questo consente di escludere dalla fattispecie tutti quei trattamenti di dati non tipicamente 'inferenziali', in cui cioè l'utilizzo di tecniche informatiche sia limitato, magari, alla conservazione e/od organizzazione di dati personali senza comportare alcun passaggio analitico e/o valutativo degli stessi. Nei trattamenti decisionali automatizzati, invece, i dati sono, al contrario, raccolti (o sottoposti alla macchina) proprio perché questa, eseguendo un dato calcolo, applicando cioè al *data-set* regole deduttive algoritmicamente definite nel programma, li analizzi per arrivare ad una certa 'soluzione', un *output* 'decisionale', appunto.

Questa decisione – perché il relativo trattamento sia rilevante ai fini e per gli

effetti della disposizione in esame, l'art. 22 del Regolamento – deve essere "basata unicamente sul trattamento automatizzato"[4]: interpretazione letterale della disposizione vorrebbe dunque che ricadano nell'ambito applicativo della esaminanda disciplina solo quelle decisioni *fully automated,* dovendosi invece ritenere escluse tutte quelle in cui sia possibile riscontrare un benché minimo coinvolgimento umano che possa variamente 'interferire' col processo decisionale automatizzato, potendo verificare o modificare la decisone ma anche, ad esempio, meramente ratificarla. Un'interpretazione siffatta, a ben vedere, rischierebbe di escludere dall'ambito applicativo della rigorosa disciplina di tutela in esame una buona parte di decisioni che sono in sostanza esito di trattamenti automatizzati ma, ad esempio, formalmente applicate per intervento umano. Molte di queste si prestano anche ad avere effetti potenzialmente molto incisivi sugli interessati; si pensi a tutti i meccanismi di '*scoring*', ampiamente utilizzati nella prassi digitale, ad esempio, per selezionare gli aspiranti ad una posizione lavorativa o valutare la probabile solvibilità di chi miri ad ottenere un fido bancario: non è raro che in questi casi gli interessati siano valutati con strumenti informatici che, applicando ai dati personali funzioni statistiche, assegnino loro un certo valore di merito, uno '*score*' appunto, e che la decisione finale, formalmente spettante ad un funzionario umano sia in realtà meramente passiva, limitandosi magari questo ad abbinare, spesso anche seguendo rigide linee guida predefinite, un certo esito ad un determinato '*score*' senza avere od esercitare alcun potere realmente 'valutativo' [5].

Tutto ciò, altrimenti vanificandosi gli scopi di tutela della esaminanda disciplina, dovrebbe più opportunamente condurre ad adottare un'interpretazione larga dell'art. 22 ritenendo incluse nella fattispecie tutte le 'decisioni automatizzate nella sostanza', anche quelle, cioè, che, benché implicanti nel processo decisionale un qualche intervento umano, questo si configuri come ininfluente rispetto al contenuto della decisione. In tal senso si esprime anche lo stesso Gruppo di Lavoro dell'articolo 29 che espressamente scrive "*The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data*" [6].

---

[4] Art. 22 (1) GDPR.

[5] Cfr. G. Malgieri, G. Comandè, *Right to legibility of automated decision-making,* in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[6] Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 21.

Prima di esso, registrava un simile orientamento anche il Garante Privacy inglese, l'Information Commissioner's Office (ICO) per cui "*the interpretation of the word "solely" in the context of Article 22(1) [...]is intended to cover those automated decision-making processes in which humans exercise no real influence on the outcome of the decision, for example where the result of the profiling or process is not assessed by a person before being formalized as a decision*" [7].

Ad ogni modo, come pure fa notare qualcuno [8], un indizio a conferma di tale interpretazione può in realtà intravedersi già nello stesso dato letterale del disposto dell'art. 22 (1) GDPR che si riferisce non a decisioni unicamente automatizzate, bensì a decisioni "*basate*" unicamente su trattamenti automatizzati: la sottile conseguenza è potersi facilmente considerare, perciò, volendo, 'letteralmente' incluse anche, quantomeno, quelle decisioni formalmente imputabili ad un agente umano ma in realtà mera applicazione passiva di valutazioni computerizzate [9].

Procedendo nell'interpretazione, queste decisioni, a norma dell'art. 22 (1) del Regolamento, oltre che basate su trattamenti automatizzati, devono pure "produrre effetti giuridici [nei confronti dell'interessato, ndr] o incidere in modo analogo significativamente sulla sua persona". L'effetto di tali decisioni deve dunque influire, negandolo o limitandolo, sul libero esercizio di un diritto della persona riconosciuto dall'ordinamento giuridico. Si pensi, e.g., al diritto a non essere discriminati in una pratica di assunzione online che non preveda intervento umano, applicazione *digital* del, anzi dei, relativi diritti previsti dalla disciplina giuslavoristica. Il catalogo di diritti potenzialmente afflitti da trattamenti decisionali automatizzati si allarga poi notevolmente tenendo da conto che questo abbraccia anche tutti quei diritti fondamentali della persona di rango costituzionale – previsti dalla nostra Costituzione come dalla Convenzione europea dei diritti umani e dalla Carta di Nizza – diritti espressi in forma aperta come la libertà di espressione, la libertà e segretezza della corrispondenza, la libertà di circolazione, di culto, il diritto di difesa e, più di tutti, il principio di non discriminazione: diritti e libertà naturalmente 'elastici', che non costituiscono cioè un *numerus clausus* ma si prestano a coprire tutta una gamma aperta di situazioni giuridiche individuali che possono essere esposte ad un concreto rischio per chi ne sia titolare a fronte di decisioni confliggenti, ed ingiuste, di un'Intelligenza Artificiale [10].

---

[7] Information Commissioner's Office, Feedback request – Profiling and automated decision-making, 2017, 19, richiamato anche in G. Malgieri, G. Comandè, *Right to legibility of automated decision-making*, in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[8] G. Malgieri, G. Comandè, *Right to legibility of automated decision-making*, in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[9] Basate cioè su un dato statistico offerto dalla macchina.

[10] Si ricorda inoltre che la stessa 'libertà informatica', come è stata autorevolmente definita,

Questa tutela ampia dei diritti della persona accordata dall'articolo in esame – e che appunto non si limita affatto al diritto alla riservatezza dei dati [11] – è ulteriormente allargata dal prosieguo della disposizione; il paragrafo 1 dell'art. 22 estende infatti la sua portata anche a quei fenomeni di ADM che pur non intaccando situazioni giuridiche soggettive apertamente qualificate come diritto "incidano [comunque, ndr] in modo analogo e significativamente sulla persona", ovverosia, nell'interpretazione che pare più consona, colpiscano, e gravino profondamente (questo il significato da attribuirsi all'espressione '*significativamente*') su interessi legittimi o comunque legittime pretese della persona umana purché non di mero fatto, ossia situazioni giuridiche che l'ordinamento, benché non riconosca come diritti immediatamente azionabili dall'individuo, ritenga ugualmente degne di protezione o accordandovi una qualche forma di tutela o quantomeno dimostrando un complessivo giudizio di riprovevolezza verso pratiche e comportamenti che ne minaccino il libero e pieno godimento individuale. Questo è il significato che a parere di chi scrive dovrebbe attribuirsi all'espressione "*incidano in modo analogo" (*"*similarly*" nella versione inglese del Regolamento), espressione che merita considerevole attenzione da parte dell'interprete perché assolutamente nuova: è infatti aggiunta *ex novo* dal GDPR accanto all'espressione "*incidano significativamente*" già presente invece nella pregressa formulazione della norma in esame, l'art. 15 dell'abrogata Direttiva 95/46/CE.

L'interpretazione proposta si spiega (e ne risulta corroborata) inoltre anche guardando al contesto politico del Regolamento sulla protezione dei dati e i suoi motivi ispiratori: se da un lato infatti, in modo lungimirante, il GDPR coglie gli enormi rischi per la persona che lo sviluppo e la diffusione di applicazioni di AI e machine learning recano con se – decidendo appunto di prevedere una tutela ampia, estesa ben oltre la privacy e fino a coprire ogni possibile diritto e libertà vulnerabile della persona – dall'altro lato, con altrettanta lungimiranza, non tra-

---

intesa in senso attivo, e cioè come libertà di valersi senza limitazioni, neppure tecnologiche come può essere una decisione automatizzata, degli strumenti informatici al servizio del proprio diritto di comunicare, trasmettere e ricevere informazioni, accedere a servizi telematici, partecipare, insomma, alla società digitale trova un suo radicato fondamento costituzionale ed esprime, per via ermeneutica, nuovi diritti soggettivi, parimenti meritevoli di tutela, da quelli tradizionalmente statuiti opportunamente adattati dall'interprete al rinnovato contesto tecnologico in cui viviamo. Sul punto V. Frosini, *L'Orizzonte giuridico di Internet,* in *Il diritto dell'informazione e dell'informatica*, n. 2, 2002, p. 275; T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Il diritto dell'informazione e dell'informatica*, n. 3, 2003, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 19 ss.; ID., *Il diritto costituzionale di accesso a Internet*, in M. Pietrangelo (a cura di), *Il diritto costituzionale di accesso a Internet*, Napoli, 2011, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 50 ss.

[11] Che pure è componente essenziale, si ricorda, del rispetto costituzionalmente sancito della libertà individuale e della dignità della persona umana. Sul punto, anche con profili comparati, T.E. Frosini, *Il diritto all'oblio e la libertà informatica,* in *Il diritto dell'informazione e dell'informatica*, n. 4/5, 2012, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 120 ss.

scura di cogliere, per converso, l'enorme potenziale espansivo per la società, l'economia e l'informazione che gli stessi strumenti tecnologici schiudono [12]: non è un caso che fin dall'art. 1 del GDPR è scritto che "*il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" ma anche "*relative alla libera circolazione di tali dati*" (pf. 1); ma ancora più significativamente al paragrafo 3, che tale "*libera circolazione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati*". In quest'ottica è ben normale che la tutela, per quanto ampia, riconosciuta dall'art. 22 trovi un limite nella proporzione, nel giusto bilanciamento, cioè, tra il libero utilizzo, nel mercato digitale, di sistemi automatizzati e le contrarie pretese soggettive che per avere tutela, o anzi per meglio dire la tutela 'più forte' di cui all'art. 22 [13] (in deroga a quella comune), è richiesto che siano legittime e, se non qualificate come diritti, quantomeno che l'ordinamento dimostri di proteggerle in modo analogo dal rischio concreto di gravi violazioni ('*significative*', ad usare il linguaggio del Regolamento).

Si lasci chiarire con un esempio; vieppiù afferente una circostanza frequentissima nel digital marketing. Non esiste nell'ordinamento un diritto a non ricevere *targeted advertising* [14], una forma cioè di marketing '*tailored*' basato sulla profilazione. Questa è una pratica perciò astrattamente lecita per quanto potenzialmente intrusiva della sfera personale; tuttavia quando la propria dimensione soggettiva risulti lesa, nel caso concreto, con un' incidenza definibile importante, sia riscontrabile cioè una certa gradazione dell'offesa – restando al caso esemplificativo, ad esempio, per l'eccessiva intrusività della raccolta dei dati [15] o per l'invasività intollerabile dei banner pubblicitari, o ancora per l'implementazione di meccanismi di *pricing* che sfruttano le specifiche debolezze dell'user per proporgli prezzi d'acquisto elevati e fuori standard – è certamente plausibile pensare che tale pratica incida significativamente e in modo analogo sull'interessato rendendosi opportuna l'applicazione della speciale disciplina di cui al-

[12] Sugli obiettivi economici collegati all'integrazione tecnologica nonché i benefici per il mercato digitale attesi quale conseguenza della maggiore 'fiducia' degli stakeholders nei sistemi di AI se opportunamente regolati in modo da garantire trasparenza, protezione dei dati e della persona umana si vadano COM (2018) 237 final, "L'intelligenza artificiale per l'Europa", pp. 9, 15-16; nonché COM (2019) 168 final "Building Trust in Human-Centric Artificial Intelligence".

[13] Come si vedrà *infra*, infatti, l'utilizzo di trattamenti automatizzati che non rientri nell'ambito dell'art. 22 è comunque soggetto alla disciplina 'comune' sulla protezione dei dati sotto il GDPR.

[14] È però previsto, proprio nel GDPR, il diritto di opporsi alla profilazione per fini di marketing. Si veda *infra*.

[15] Si pensi ai casi di tracking dell'utente attraverso più siti web, magari anche attraverso più devices, per ricavarne preferenze e interessi.

l'art. 22 GDPR (che, come si vedrà, richiede necessariamente, tra le altre cose, ad esempio, il consenso informato dell'interessato: v. *infra*). Ciò in ragione non della violazione di un preciso diritto dell'interessato, ma per via dell'esistenza, comunque, nel caso in questione, di una sua legittima pretesa (ricavabile dal complesso dell'ordinamento) a non essere vittima di pratiche commerciali scorrette o essere manipolato nel formarsi di una sua adesione alla volontà di acquistare un determinato bene [16]; nel caso del *pricing*, anche una sua aspettativa a non essere oggetto di pratiche potenzialmente lesive di *price-discrimination* [17]. Volendo fare un altro esempio, il generale principio di correttezza e non discriminazione, ancora, è alla base della legittima pretesa degli interessati a non vedersi rifiutata con processi automatizzati una domanda di credito online: quest'ultima è un'altra tipica ipotesi di ADM rilevante per l'art. 22, per di più autorevolmente citata esemplificativamente dallo stesso Considerando 71 del Regolamento.

4. Una disciplina 'comune' dei trattamenti automatizzati

Pur interpretando in senso ampio la fattispecie di cui all'art. 22 GDPR, ovviamente non tutti i trattamenti di dati che siano condotti con sistemi informatici o di Intelligenza Artificiale finiscono con l'esservi riconducibili; quantomeno quei trattamenti (marginali) che prevedono nel processo decisionale un significativo intervento dell'uomo (accanto a sistemi di raccolta, analisi e conservazione automatizzata dei dati) rifuggono l'applicazione della rigorosa disciplina che si sta esaminando.

Mentre i trattamenti decisionali automatizzati di cui all'art. 22 sono consentiti solo nelle ipotesi di cui al paragrafo 2, gli altri restano ammissibili, tanto per cominciare, in tutti i casi in cui il trattamento dei dati è considerato lecito a norma dell'art. 6 GDPR (ovvero alle condizioni di cui alle lettere dalla a alla f di detto articolo).

Le speciali salvaguardie che il paragrafo 3 dell'art. 22 impone ai titolari di quei trattamenti non sono qui richieste, in primis l'intervento umano.

Trovano applicazione, tuttavia, nei confronti di ogni trattamento di dati personali condotto con sistemi informatici (ricada o no nell'ambito dell'art. 22) quelli che sono i principi generali del GDPR: può parlarsi a riguardo di una disciplina "comune".

---

[16] Principio che l'ordinamento normalmente prevede, ad esempio, a presidio del consumatore in tutte le ipotesi di acquisto a distanza o fuori dai locali commerciali.

[17] Si pensi a meccanismi di dynamic-pricing che, viziati da *bias*, propongano all'utente prezzi troppo elevati col risultato gravoso di escluderlo dall'accesso equo a determinati beni o servizi.

Tra questi principi generali troviamo, in primis, quello di liceità, correttezza e trasparenza del trattamento (art. 5 (1) (a)); a quest'ultima condizione fanno da pendant il diritto dell'interessato ad essere adeguatamente informato circa il trattamento che lo riguarda e ad essere edotto di tutte le circostanze indicate, a seconda del caso, dagli artt. 13 e 14 (diritto all'informativa) ovvero 15 (diritto di accesso). Seppur non tenuto ai più pregnanti oneri informativi di cui meglio si dirà nel prosieguo e che riguarda il solo caso dei trattamenti *ex* art. 22, il responsabile del trattamento è tenuto in ogni caso a fornire all'interessato un'informativa concisa, trasparente, intellegibile e facilmente accessibile, fornita con linguaggio semplice e chiaro e anche, eventualmente, circostanza importante data la materia di cui ci si occupa, in forma elettronica.

Di specifica rilevanza il principio di correttezza: le tecniche di *Big Data* e profilazione, ad esempio, possono ben facilmente, per bug di programmazione o anche semplicemente perché applicate a data-set incompleti o dati inesatti, condurre a decisioni discriminatorie (si pensi ai rischi connessi a sistemi informatici correntemente utilizzati per la selezione delle risorse umane o per valutare richieste di accesso al credito online, calcolare premi assicurativi in base ai potenziali fattori di rischio, ecc.).

A tale principio si riconnettono quello di accuratezza, esattezza e aggiornamento dei dati (art. 5 (1)(d) GDPR), cui simmetricamente si rifanno i diritti dell'interessato alla rettifica (art. 16), alla cancellazione dei dati (art. 17) e alla limitazione del trattamento (art. 18). L'obbligo per i titolari del trattamento di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (art. 5 (1)(d) GDPR) e gli accennati diritti di 'autotutela' dell'interessato, che ne garantiscono il controllo sull'accuratezza dei dati coinvolti, nel trattamento assumono notevole importanza nell'ambito dei trattamenti automatizzati e ciò per gli enormi rischi che trattamenti di *data-analysis* possano essere viziati da *bias* e condurre a risultati di rilevante impatto per i soggetti coinvolti [18]. Tali rischi sono ancora maggiori quando ci si trovi davanti a sistemi informatici deduttivi come quelli di *Big Data analytics* o *profiling*, capaci di estrapolare, analizzandoli e mettendoli in correlazione statistica, dati da dati, ampliando esponenzialmente i rischi di scarsa accuratezza del data-set, alla cui qualità e precisione è, ovviamente, inversamente proporzionale il rischio di *machine bias (o algorithmic bias)* ovvero di deduzioni errate da parte di AI *systems* dotati di autonomia decisionale [19].

---

[18] Per approfondire, cfr. G. D'Acquisto, *Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, in F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

[19] Cfr G. D'Acquisto, *op. cit.*

Assumono una peculiare importanza anche i principi, pure questi di generale applicazione, di limitazione delle finalità di trattamento, minimizzazione dei dati e limitazione della loro conservazione (rispettivamente *ex* art. 5(1)(b)(c)(e)GDPR). La normale attitudine dei sistemi appena enunciati a processare enormi quantità di dati, spesso anche originariamente raccolti per scopi diversi da quelli per cui sono trattati [20] rende di assoluta importanza l'obbligo del titolare del trattamento di raccogliere i dati per finalità determinate ed esplicite, limitando il trattamento a quei dati che siano pertinenti e assolutamente necessari rispetto alle finalità per cui sono trattati; come pure, altrettanto rilevante, è l'imposta necessità di conservarli, con mezzi adeguati e sicuri, per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati, dovendo pure essere esplicitata in modo chiaro l'eventualità di una loro possibile trasmissione a terzi.

Di particolare interesse, parlando di trattamenti condotti attraverso applicazioni di IA, è anche il diritto di opposizione (art. 21 GDPR), soprattutto per la previsione di cui al paragrafo 2 per la quale in caso di dati trattati per finalità di marketing diretto (una delle applicazioni più comuni del profiling) l'opposizione dell'interessato determina l'immediata e definitiva cessazione del trattamento non essendo neppure ammesso, unico caso, il titolare a provare l'eventuale esistenza di ragioni che giustifichino la prevalenza del suo legittimo interesse a proseguire il trattamento [21].

5. Il diritto alla 'intelligibilità' dell'algoritmo: un'interpretazione sistematica e coerente del GDPR

Se quella appena analizzata è la disciplina applicabile ad ogni forma di trattamento dei dati condotta con tecniche automatizzate, è solo ai trattamenti decisionali automatizzati (o ADM) rilevanti ai sensi dell'art. 22 GDPR che si applica invece quella specifica e più rigorosa disciplina sulla trasparenza dell'algoritmo contenuta negli artt. 13 (2)(f),14 (2)(g) e 15 (1)(h) del Regolamento.

Le disposizioni citate, con formulazione identica, prevedono – nel caso degli artt. 13 e 14 nell'ambito dell'informativa, nel caso dell'art. 15 quale contenuto del diritto di accesso – che "l'interessato ha il diritto di essere informato circa l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, [a ricevere, ndr] informa-

[20] Si pensi alla profilazione operata a fini di targeted marketing sulla base di dati personali variamente raccolti in merito ai gusti e alle abitudini di un utente sulla rete.

[21] La norma è una novità introdotta col GDPR; lascia trapelare un giudizio di notevole pericolosità da parte del legislatore europeo nei confronti di questa pratica commerciale cui contrappone quale rimedio una forma di tutela assoluta della persona.

zioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

Sebbene non poche delle interpretazioni della disposizione citata emerse in dottrina, improntate a forte cautela, ritengono di limitare la portata dell'onere in questione per il titolare del trattamento ad una semplice informativa all'interessato circa l'esistenza di un trattamento decisionale automatizzato [22] idoneo a produrre effetti nei suoi confronti o comunque ad incidere significativamente sulla sua sfera giuridica, è di tutta evidenza come invece il diritto in questione non possa che riferirsi ad un *quid pluris*, il contenuto di detta informativa non sarebbe altrimenti in nulla diverso da quello già comunque dovuto per ogni altro trattamento del dato rendendosi del tutto superflua la specificazione invece espressamente voluta dal legislatore europeo.

Vieppiù, la disposizione in esame esplicitamente aggiunge alla mera notifica di 'esistenza' del processo automatizzato il dovere del titolare del trattamento di fornire *anche* informazioni *aggiuntive* (significativo proprio l'uso della congiunzione *e,* proprio a segnare qualcosa di diverso e *in più*) "almeno in tali casi" – ovvero i trattamenti decisionali di cui all'art. 22, altra prova di una ultroneità del requisito informativo richiesto giustificato proprio dalla particolarità della fattispecie – che siano "significative" sulla "logica" utilizzata dall'algoritmo applicato al trattamento, nonché "l'importanza e le conseguenze previste di tale trattamento per l'interessato". È dunque fuori di dubbio che si tratti di un dovere d'informazione certamente più pregnante di quello normalmente previsto per gli altri trattamenti di dati personali.

Quanto al contenuto, invece, di questo 'diritto conoscitivo' dell'interessato occorre, a parere di chi scrive, operare una distinzione tra l'informazione dovuta ai sensi degli artt. 13 (2)(f) e 14 (2)(g) e quella dovuta quale conseguenza dell'esercizio del diritto di accesso dell'interessato ai sensi dell'art. 15 (1)(h) GDPR.

A dispetto di una formulazione pressoché identica delle disposizioni, infatti – come fatto notare in modo efficacemente argomentato da certa dottrina [23] – mentre nell'ambito dell'informativa le informazioni dovute non possono che riferirsi alla generale funzionalità dell'algoritmo e al tipo di decisioni normalmente attese dal suo funzionamento con valutazione astratta ed *ex ante*, nel caso del diritto d'accesso è più opportuno interpretare la norma traendone un dovere di informazione del titolare del trattamento più pregnante e dettagliato e che attenga alla specifica decisione eventualmente già adottata dal sistema nei confronti

[22] S. Watcher, B. Mittlestadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the GDPR*, in *International Data Privacy Law*, vol. 7, 2017, p. 76 ss.

[23] G. Malgieri *et al.*, *op. cit.*

dell'interessato e i passaggi inferenziali che hanno portato la macchina a quel dato output.

La necessità di un'interpretazione tal fatta è la naturale conseguenza di un'interpretazione sistematica e coerente del paragrafo 1, lett. h) dell'art. 15 del Regolamento. Come già visto, infatti, l'art. 22 GDPR, al paragrafo 3, prevede espressamente il diritto dell'interessato destinatario di una misura di ADM a mettere in discussione la decisione automatizzata attraverso la possibilità di ottenere l'intervento umano e cioè di relazionarsi in modo 'dialettico' col titolare del trattamento esprimendo la propria opinione, chiedendo di procedere ad una verifica della decisione e potendo anche, successivamente, contestarne gli assunti. Si tratta di un diritto, a ben vedere, che, salvo a volerne frustrare il contenuto sostanziale, sottende necessariamente, da parte dell'interessato (e quindi richiede al titolare del trattamento) un'informazione specifica sul funzionamento dell'algoritmo, non astratta e pronostica ma concreta ed *ex post,* calata nell'applicazione specifica che lo riguarda; solo in tal modo infatti l'interessato sarebbe messo in condizione di esercitare appieno il suo diritto oppositivo, disponendo degli strumenti idonei a muovere una contestazione specifica e motivata. Non è un caso infatti - a parere di chi scrive – che il Considerando 71 al Regolamento espressamente metta in relazione questi due diritti dell'interessato elencando, tra le garanzie opportune che si dovrebbero accompagnare a trattamenti decisionali automatizzati, "la specifica informazione dell'interessato e il diritto di ottenere l'intervento umano [...]", parlando, per di più, significativamente, proprio di "un'informazione *specifica*" [24].

Nello stesso senso si è espresso lo High Level Expert Group on Artificial Intelligence (AI HLEG), gruppo di esperti istituito dalla Commissione europea con le Comunicazioni del 25 aprile e del 7 dicembre 2018 con lo specifico compito di individuare, nel quadro dei valori e dei principi giuridici dell'UE, precisi orientamenti etici atti a governare uno sviluppo socialmente sostenibile dell'Intelligenza Artificiale. Nel documento pubblicato il 8 aprile 2019, e significativamente intitolato "Orientamenti Etici per un'IA affidabile", il consesso, dopo aver individuato una serie di principi fondamentali, tra cui l'equità, cui il nuovo quadro tecnologico dovrebbe informarsi per essere "*trustworthy*", cioè per far sì che gli esseri umani e le comunità possano riporvi fiducia ed affidarsi all'uso delle nuove applicazioni tecnologiche dando così slancio al mercato digitale con tutti i benefici espansivi che comporta, significativamente afferma: "*La dimen-*

[24] Interpretazione diversa, va segnalato, propone nelle *Linee guida* il WP29 per cui l'onore informativo *ex* art. 15 (1)(h) GDPR dovrebbe consistere in una "*information about the envisaged consequences of the processing rather than an explanation of a particular decision".* Cfr. Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 27.

sione procedurale dell'equità implica la capacità di impugnare le decisioni elaborate dai sistemi di AI […] *e la possibilità di presentare un ricorso efficace contro di esse. A tal fine* […] *i processi decisionali devono essere spiegabili*". Ivi, ancora, più specificatamente sull'esplicabilità, si aggiunge: "*Tale principio implica che i processi devono essere trasparenti, le capacità e lo scopo dei sistemi di AI devono essere comunicati apertamente e le decisioni, per quanto possibile, devono poter essere spiegate a coloro che ne sono direttamente o indirettamente interessati. Senza tali informazioni una decisione non può essere debitamente impugnata*" [25].

Ultimo punto che resta da affrontare è cosa si intenda per "informazioni significative sulla logica utilizzata, l'importanza e le conseguenze previste di tale trattamento per l'interessato". È opinione di chi scrive che, alla luce di un'interpretazione che, anche in questo caso, guardi al contesto delle disposizioni regolamentari – in particolare ai requisiti di chiarezza, intelligibilità, accessibilità, semplicità di linguaggio che presidiano all'informazione cui ha diritto in via generale l'interessato soggetto a un trattamento dei propri dati personali *ex* art. 12 (1) GDPR – deve escludersi che il legislatore europeo voglia riferirsi ad un obbligo di mera 'trasparenza' dell'algoritmo, soprattutto se inteso nella sua veste matematica come cioè architettura di sistema, dovendosi piuttosto ritenere che quello che qui interessa, e compete al titolare del trattamento esplicare – magari in aggiunta alla funzione matematica che sostanzia l'algoritmo in questione – è la sua concreta implementazione: il contesto in cui è applicato, gli scopi perseguiti, le tecniche applicate e magari anche degli esempi circa il suo concreto funzionamento. Solo allegando tali circostanze all'informativa dovrebbe potersi ritenere assolto quel dovere "esplicativo" che il legislatore sembrerebbe richiedere.

Alla luce di ciò, ecco spiegato perché [26] si è voluto connotare il diritto dell'interessato di cui agli artt. 13 (2)(f),14 (2)(g) e 15 (1)(h) del Regolamento come un diritto alla 'intellegibilità' dell'algoritmo, volendosi in qualche modo, con tale espressione, tradurre quella di '*legibility*' usata per la prima volta da Richard Mortier [27] proprio per riferirsi ad una *disclosure* dell'algoritmo che riassumesse la trasparenza del programma unitamente alla comprensibilità del suo funzionamento da parte degli individui ad esso soggetti o potenzialmente interessati dal suo funzionamento.

---

[25] *Ethics guidelines for trustworthy AI* (AI HLEG), 2019, paragrafi 52 e 53. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[26] Anche sulla scorta e l'intuizione di G. Malgieri *et al.*, *op. cit.*

[27] R. Mortier *et al.*, *Human data interaction: The human face of the data-driven society*, in *MIT Technology Review*, 2014.

6. L'Accountability, l'obbligo di DPIA e il ruolo della privacy by design e by default nel futuro di una data-driven society

Un ultimo aspetto su cui vale la pena soffermarsi, fisiologicamente in conclusione di questa breve trattazione, è l'accountability, ovvero il principio di responsabilizzazione del titolare del trattamento per cui quest'ultimo, ai sensi dell'art. 5 (2) GDPR, è chiamato a comprovare il rispetto delle norme sulla protezione dei dati.

È in questa sede infatti che il titolare del trattamento, stando all'art. 24 del Regolamento - tenuto conto della natura, del contesto e delle finalità del trattamento, valutati pure tutti i rischi ad esso contestuali per i diritti e le libertà individuali – è tenuto a dimostrare che il trattamento è effettuato in modo conforme al GDPR e cioè che sono rispettati tutti i principi e le condizioni, anche specifiche, che informano il trattamento dei dati e che tutti i diritti stabiliti dalla legge a presidio degli interessati, attuali o potenziali, sono adeguatamente garantiti. Il titolare del trattamento – prima di procedere allo stesso come pure, periodicamente, nel corso di questo – deve individuare il tipo di trattamento che si appresta ad eseguire, i dati e i soggetti coinvolti, valutarne la probabilità e la gravità dei rischi e dar prova di aver diligentemente ottemperato a tutti gli obblighi di protezione del caso.

È in punto di accountability, ad esempio, che, ove il trattamento importi processi automatizzati, il titolare deve provare che questo non ricada nell'ambito dell'art. 22 ove non voglia o non possa rispettarne le condizioni; viceversa, laddove ritenga si tratti di ADM basato unicamente su trattamenti automatizzati, è sempre in questo contesto che deve dimostrare di aver adempiuto a tutti gli oneri informativi richiesti dal Regolamento e adottato misure di salvaguardia adeguate.

Si tenga anche presente che, ai sensi dell'articolo 35 del GDPR, "quando il trattamento prevede l'uso [...] di nuove tecnologie" e "può presentare un rischio elevato per i diritti e le libertà della persona fisica" il titolare del trattamento è pure obbligato a svolgere (consultandosi col DPO, ove nominato) una specifica valutazione di impatto del trattamento sulla protezione dei dati (o DPIA); essa è peraltro in ogni caso obbligatoria (ai sensi del paragrafo 3 dell'art. 35) quando si pongano in essere "trattamenti che comportano una valutazione globale e sistematica degli aspetti relativi alle persone fisiche, basate su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche" [28].

[28] Si evidenzia che la disposizione citata discorre di decisioni "basate su" trattamenti automa-

Ai fini di questa valutazione un *auditing* dell'algoritmo, una cioè chiara esplicazione del suo funzionamento risulta non solo strumentale a quell'onere suddetto di 'intellegibilità' del processo automatizzato – prevista a beneficio dei soggetti interessati - ma è pure essenziale al titolare del trattamento proprio per assolvere al suo impegno di accountability: solo esplicando nel dettaglio il funzionamento dei processi decisionali automatizzati che governano il trattamento questi potrà comprovare il rispetto del GDPR [29], ben difficilmente potendosi immaginare che un black-box algorithm – perché tenuto volontariamente segreto o perché magari dal funzionamento addirittura non prevedibile nei suoi concreti esiti neppure da chi lo abbia predisposto o implementato – sia idoneo ad assicurare, tanto per fare un esempio, il rispetto della limitazione del trattamento o la minimizzazione della raccolta dei dati.

È importante ricordare, inoltre, che il titolare del trattamento non può limitarsi ad assolvere gli oneri cd. informativi, o garantire i diritti dell'interessato che sia soggetto al trattamento automatizzato; a norma dell'art. 24 del Regolamento esso è tenuto pure ad 'attivarsi' mettendo in atto misure tecniche e organizzative adeguate al caso concreto per garantire la *compliance* al GDPR, e questo è un obbligo che richiede non solo una *disclosure* dell'algoritmo ma anche, a monte, una corretta predisposizione o selezione degli strumenti di Intelligenza artificiale più adatti ad assicurare una corretta protezione dei dati personali e dei diritti e delle libertà dei soggetti coinvolti. Le metodologie cui il titolare del trattamento ricorre a tal fine sono quelle di cui all'art. 25 del Regolamento della privacy by design e by default, ovvero, con l'improvvida traduzione italiana, della protezione dei dati fin dalla progettazione e per impostazione predefinita.

La pianificazione delle misure tecniche da applicarsi ad uno specifico trattamento e alle sue particolari criticità in modo da minimizzarne i rischi (privacy by design) e ancor di più la corretta ideazione e definizione, a monte, degli strumenti e delle applicazioni informatiche da adoprarsi per il trattamento in modo da garantire che, per impostazione predefinita, sia *privacy-compliant* (privacy by default), acquistano quindi, nell'humus di questa sempre più *data-driven society* un ruolo di primissimo piano rappresentando lo strumento principe in grado di raccogliere la sfida del futuro della protezione dei dati come pure del mercato digitale [30]: chiunque voglia servirsi di applicazioni di AI, Big Data

---

tizzati e non invece di decisioni "basate unicamente su" trattamenti automatizzati, con la conseguenza che la fattispecie copre, ma è più ampia di quella *ex* art. 22 (1) GDPR. Cfr. Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 29.

[29] Per approfondire v. G. Malgieri *et al.*, *op. cit.*

[30] Su come il modello di accountability del GDPR e gli strumenti di privacy by design possano assurgere a modello efficace per la gestione computazionale ed automatizzata dei vari profili di

Analytics, IoT ecc. o anche solo offrire tali servizi sul mercato dovrà fare i conti con l'accountability del GDPR – direttamente i titolari del trattamento, indirettamente gli informatici, sviluppatori e produttori di questi sistemi – tutti chiamati a sforzarsi di costruire sistemi non solo tecnologicamente evolutivi ma sempre più *privacy-compliant*, progettati per assolvere efficacemente a determinate finalità pratiche ma pur sempre in modo da garantire il rispetto non solo delle regole sulla protezione dei dati a più in generale dei diritti e delle libertà della persona che ne possano risultare minacciati [31].

7. Impressioni conclusive

Il GDPR, dunque, concludendo, non vuole porre un limite alla tecnologia, ma piuttosto indicare una direzione o, meglio ancora, un binario entro il quale questa è libera di correre, sempre più veloce, senza deragliare nella violazione dei diritti umani o incrociare la corsa con le libertà fondamentali dell'individuo, ma piuttosto mettendo al servizio di queste la sua velocità in una comune corsa al futuro (e ci si augura, per il meglio). E mentre si è già in arrivo alla prossima stazione, e la fantasia diventa ingegneria, già si immaginano (e costruiscono) i primi sistemi di machine learning che, interiorizzati principi etico-giuridici, siano in grado di assumere in autonomia tutte le scelte procedimentali più opportune per adeguare, dinamicamente ed in modo automatico, il trattamento alle via via emergenti necessità di tutela degli interessati. Funzionerà? A giudici robot l'ardua sentenza.

responsabilità civile dei robot e delle AI technologies si legga G. Comandé, *Responsabilità ed accountability nell'era dell'Intelligenza Artificiale,* in Di Ciommo, Troiano (a cura di), *Giurisprudenza e Autorità Indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, p. 1001 ss.; su come principi etico-giuridici possano, e debbano, essere implementati nella progettazione dei sistemi di AI, una sorta di *Ethics by design*, cfr. *Ethics guidelines for trustworthy AI* (AI HLEG), 2019, paragrafo 98. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[31] Per approfondire, F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

SMART CONTRACTS IN THE BLOCKCHAIN CONTEXT: WHAT HAPPENS?

Veronica Carriero

Abstract:

Thanks to the blockchain technology, the idea of an entire computer regulated contract has become a reality. However, only a careful study of the performance of this new contractual model will disclose all its advantage.

Key-words: Smart contracts

Summary: 1. Introduction. – 2. Smart contract and blockchain. – 3. Smart contract as a contractual model.

1. Introduction

The term "smart contracts" was created in the 1990s by Nick Szabo, a computer scientist, who defined it as a series of digitally fixed promises included in a protocol, with whose help the parties observe their commitments. The idea of Szabo was to enter into a contract that is completely monitored by a computer and without the assistance of agents [1]. It has been pointed out [2] that "the concept remained obscure for lack of the right technology" [3]. In recent years, especially by developing the blockchain technology, there has been a rebirth of the concept. The idea of smart contracts can be examined both in a broad sense and in a narrow sense. According to the first approach, a smart contract is deemed to be as a self-executing, computerized "if-then" relationship based on blockchain technology and with legal implications. According to the second one, any com-

[1] M. Fries, B.P. Paal (eds.), *Smart contracts*, Mohr Siebeck, Tübingen, 2019, 1.

[2] 'Not so clever contracts. For the time being at least, human judgement is still a better bet than cold-hearted code' [2016] The Economist (online).

[3] For further studies on the evolution of technological society and the informatic freedom see T.E. Frosini, *Liberté, egalité, internet*, Editoriale scientifica Naples, 2019.

puterized "if-then" relationship can be defined as smart contract, regardless of the deployment of blockchain technology [3].

2. Smart contract and blockchain

There are plenty of definitions for the blockchain, an efficient one is "a data storage system using linked sequential chunks of information. It is literally a chain of blocks designed to create an immutable ledger of transactions" [4]. This technology is capable of being used for many purposes including the creation and execution of smart contracts. The blockchain technology would implement the idea of an entire computer regulated contract, with no human intermediation. The fortune of the blockchain technology [5] lies in its special features. The mechanism is based on a process called "consensus" that regulates how information can be added to the shared storage in an orderly manner and by which "basic function of blockchains is to reliably share information among parties who may not trust one another. In other words, everyone can have his or her copy of a ledger and trust that all those copies remain the same, even without a central administrator or master version" [6]. Furthermore the system is distributed to the effect that every single node has a complete and accurate copy of the blockchain and there is no central control point [7]. Another trait is the autonomy: the blockchain technology relies on a peer-to-peer network and this fosters the execution of computer code in a manner that is independent of any one party [8]. The system is also immutable, resilient and tamper resistant: once information has been recorded to a blockchain it becomes immutable or at least exceptionally hard to change or delete because no single party has the power to modify or restore information saved on a blockchain or to shut down the execution of a smart contract once it has been implemented, unless allowed by the code [9]. Cryptocurrency based on the blockchain system ensures there is only one ledger with no contradictions by using a technique called "proof of work" that allows

[3] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1.

[4] K. Werbach, *The Blockchain and the New Architecture of Trust*, MIT Press, 2018, 14.

[5] On the advantages of the blockchain technology in business *see* 'The promise of the blockchain technology. What blockchains may be able to do for your business, and what they can't' [2018] The Economist (online).

[6] K. Werbach, *The Blockchain*, n. 4, 7.

[7] K. Werbach, *The Blockchain*, n. 4, 96.

[8] P. De Filippi, A. Wright, *Blockchain and the Law. The Rule of Code*, Harvard University Press, 2018, 43.

[9] P. De Filippi, A. Wright, *Blockchain*, n. 8, 35.

the blockchain to be stored on every computer in the network at the same time and provides that each copy of the blockchain will be identical [10]. The information recorded is transparent and nonrepudiable in that anyone can download the entire blockchain and once a transaction occurs on a blockchain-based system, parties will find it difficult to refuse their involvement [11]. Furthermore, blockchain makes it possible for a person to store data or to carry out operations without revealing one's true identity because the system relies on digital signatures and key cryptography [12].

It has been pointed out [13] that in the life cycle of a blockchain-based smart contract there are different stages. The first one is the creation of the contract and in this phase it is defined and translated into a code. The second stage consists in "freezing" the software and adding it to the chain. The third step is the execution one: the software is read and implemented by the nodes. Finally, the smart contract is completed, information and transaction are recorded on the blockchain and the consensus protocol is validated.

3. Smart contract as a contractual model

Legal scholars have focused their attention on the legal nature, status and implications of the described mechanism. According to an authoritative doctrine [14], the position of a smart contract users is similar to the position of a receiver of "terms and conditions of a contract". Another approach [15] assumes that smart contract consists in a computer code with a contractual value.

It has been highlighted [16] that, unlike other contracts, a smart contract has a greater legal certainty and could ensure better that the outcome of the operation responds to the expectations of the parties. Furthermore, the smart contract can reduce the transaction costs, doubts of interpretation and increase the speed in the conclusion of the contract. Advantages would exist also in terms of trans-

[10] A. Rothstein, *The end of money. The story of bitcoin, cryptocurrencies, and the blockchain revolution*, Nicholas Brealey Publishing Boston, 2017, 43.

[11] P. De Filippi, A. Wright, *Blockchain*, n. 8, 37.

[12] P. De Filippi, A. Wright, *Blockchain*, n. 8, 38.

[13] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1, 4.

[14] R. Pardolesi, A. Davola, '«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia", 2019, 4, 195 ff.

[15] The Author reports a "technologic neutral" point of view: "*Aus technologieneutraler Sicht betrachtet versteht man hier den Smart Contract als Computercode mit vertragsrechtlicher Bedeutung*" in M. Fries, B.P. Paal (eds.), *Smart contracts*, p. 5.

[16] M. Fries, B.P. Paal (eds.), *Smart contracts*, *ivi*, p. 7 ff.

parency, traceability and monitorability of the transactions. The same Author points out that these smart contracts are neither "smart" nor "contracts". Smart contracts would not be smart because they are not capable to understand the language and they are not capable to assess in an independent manner external events that affect the execution of the contract: in this case is required a trusted third party source, commonly referred to as an "oracle", by which the blockchain system can interact with real world and react to external events. Moreover, smart contracts could not be defined as contracts in the technical sense: they consist in a sequence of orders incapable to take into account the environment and external facts which affect the process [17].

Regarding the weaknesses of a blockchain-based smart contract, one should consider that the described system ignores all the nuances of the language and this is all the more apparent in the open-ended contractual terms that outline performance obligation such as to act in "good faith" or to use "best efforts" to fulfil the obligations because it might be hard to define what is appropriate performance or because the most efficient manner of performance might not yet be predictable. "Act of God" as legal term cannot be translated into a code. It has been highlighted that open ended or ambiguous contractual provisions may result in more efficient contracts [18]. Furthermore, any undesirable transaction cannot be reversed nor is it possible to adapt the content of the agreement in case of external event modification, once the contract is effective [19]. It is possible that the best way to use this mechanism would be to create hybrid arrangements that combine natural language terms with smart contract translated in a code [20]. In conclusion, a smart contract is certainly a model of great interest and only a careful study of the performance practice of this model will reveal how to take full advantage of its capabilities.

[17] *Idem.*

[18] P. De Filippi, A. Wright, *Blockchain*, n. 8, p. 77 and note 24 for the source.

[19] M. Fries, B.P. Paal (eds.), *Smart contracts*, n. 1, 10.

[20] P. De Filippi, A. Wright, *Blockchain*, n. 8, 78.

IL TRATTAMENTO ILLECITO DI DATI PERSONALI IN AMBITO PROCESSUALE

Mariní Gaia Chiacchio

Keyword: Trattamento illecito di dati personali – dati sensibili – condizioni obiettive di punibilità

Case: Cass. pen., sez. III, 29.5.2019, n. 23808

Summary: 1. Il fatto. – 2. Il trattamento illecito di dati personali: struttura ed analisi normativa. – 3. Brevi cenni sulle c.d. "condizioni obbiettive di punibilità": la natura giuridica del nocumento. – 4. Le conclusioni adottate dalla Cassazione e osservazioni conclusive.

1. La Sez. III penale n. 23808 della Corte di Cassazione, in data 29 maggio 2019, ha confermato la pronuncia della Corte di Appello di Firenze [1], assolvendo dal delitto *ex* art. 167 d.lgs. 196/2003 il sig. Claudio A.

Egli, invero, era stato denunciato da figlio Paolo A. per aver diffuso, nell'ambito di un procedimento civile, senza il consenso dell'avente diritto, dati sensibili attinenti lo stato di salute del ricorrente.

Questi ultimi, in particolare, concernevano una documentazione sanitaria relativa ad una grave patologia psichiatrica ritenuta, a detta dell'imputato, alla base dell'atteggiamento di profondo risentimento avverso i genitori manifestato dal ricorrente, tale da portare lo stesso, in un giudizio civile, a rivendicare verso il convenuto specifici crediti.

Ebbene, a detta della parte attorea, suddetta diffusione aveva comportato non solo un danno non patrimoniale, causato dalla diffusione di dati afferenti la sfera intima della vittima ma, altresì, un danno patrimoniale per aver indotto lo

[1] Trattasi, più nello specifico, di una pronuncia della Corte di Appello di Firenze datata 20 aprile 2018 la quale ha riformato la decisione del Tribunale di Arezzo in data 26 febbraio 2014.

stesso ad addivenire ad una transazione, nonché per aver ostacolato il reinserimento del soggetto *de quo* nel mondo del lavoro in seguito alla diffusione di informazioni sensibili nei confronti di una platea indefinita di soggetti quali giudici, cancellieri, avvocati e praticanti.

Ciò malgrado, i giudici di Piazza Cavour hanno dichiarato il ricorso inammissibile.

Infatti, sebbene la produzione della documentazione in sede processuale fosse avvenuta in violazione dei limiti del diritto di difesa richiesti *ex lege,* quali i doveri di correttezza, pertinenza e non eccedenza (in quanto ultronea rispetto agli altri argomenti spesi per negare la sussistenza del credito), la Corte ha escluso la sussistenza del nocumento.

Invero, nonostante le modifiche apportate all'art. 167 dal d.lgs. 101/2018, il requisito *de quo* è tuttora richiesto ai fini della configurabilità del fatto di reato.

Pertanto, per meglio comprendere il caso in analisi, nonché la soluzione adottata dalla Suprema Corte di Cassazione, risulta preliminarmente necessario analizzare in breve la struttura dell'art. 167, d.lgs. 193/2016, soffermandosi poi sul concetto di "nocumento"[2] richiesto dallo stesso in quanto elemento costitutivo del fatto.

2. Il trattamento illecito dei dati personali, disciplinato dall'art. 167 del d.lgs 193/2016[3], è un reato comune e a dolo specifico, caratterizzato da una clausola di riserva espressa, evidente nella locuzione e «salvo che il fatto non costituisca più grave reato»[4].

---

[2] Risulta in particolare necessario rilevare che la Corte, richiamando, peraltro, quanto statuito in passato dalla Sez. 3, n. 29549/2017, ha chiarito che il nocumento richiesto ai sensi dell'art. 167 in esame è costituito dal pregiudizio, anche di natura non patrimoniale, subito dalla persona cui si riferiscono i dati quale conseguenza dell'illecito trattamento.

[3] Per un approfondimento v. M. SALA, *Guida alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del codice della privacy italiano,* Torino, 2018.

[4] In seguito alle modifiche apportate dal d.lgs. n. 101/2018, l'art. 167 dispone che: «1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento

Con maggior impegno esplicativo, la fattispecie *de qua* rientra nelle c.d. "norme miste cumulative", in quanto disciplina reati autonomi, caratterizzati da una propria cornice edittale. Logica conseguenza di siffatta peculiarità è che, nell'ipotesi in cui siano realizzate più condotte, si andrà a configurare una pluralità di reati in concorso reale [5].

Per vero, per meglio analizzare l'articolo oggetto di tale disamina risulta necessario soffermarsi, seppur brevemente, sui singoli commi che lo compongono.

Il **comma I** delinea un reato c.d. "a consumazione anticipata". Qui, infatti, la condotta (che consiste nell'operare in violazione delle disposizioni in materia di comunicazioni elettroniche) deve necessariamente arrecare un nocumento sorretto dalla volontà di ottenere un profitto provocando un danno all'interessato. Peraltro, i generici rimandi agli artt. artt. 123, 126, 130 e ai provvedimenti di cui all'art.129 inducono a definire la fattispecie *de qua* una norma c.d. "parzialmente in bianco" [6].

Il **comma II**, rilevante ai fini di siffatta disamina, prevede un'ulteriore fattispecie, punita più gravemente.

In tal caso la condotta, infatti, consiste nel trattare dati particolarmente sensibili, relativi a condanne penali e reati, in violazione di legge, regolamento e delle misure di garanzia, al fine di trarre profitto ovvero di arrecare danno.

Qui il dolo specifico è previsto nella forma alternativa, poiché la condotta può arrecare, altresì, un nocumento.

A tal proposito, risulta necessario da subito specificare che danno e nocumento costituiscono due concetti dalla differente portata applicativa. Il nocumento, invero, è (anche solo) un mero pregiudizio.

Per completezza, circa l'elemento soggettivo, il Garante, come si legge nel Dossier relativo ai lavori parlamentari, suggerisce «*di considerare, quale oggetto alternativo del dolo specifico, anche il nocumento, in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore,*

---

all'interessato. 4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante. 5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto. 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita».

[5] Le norme c.d. "miste cumulative" vanno distinte dalle norme c.d. "miste alternative". Queste ultime si realizzano allorquando all'interno del medesimo articolo è possibile rinvenire un unico reato realizzabile mediante plurime condotte. In tale ipotesi, pertanto, la fattispecie criminosa sarà applicabile una sola volta in caso di realizzazione contestuale di tutte le condotte tipizzate. V. F. Garofoli, *Manuale di diritto penale parte generale*, 2014, Roma, 1229.

[6] Sulla disciplina delle c.d. "norme penali in bianco" v. F. Garofoli, *op. cit.*, 81.

anche quando sorrette dal dolo di danno e non solo da quello di profitto. Tale modifica consentirebbe di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'abolitio crìminis che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta» [7].

Al **comma III** la condotta si sostanzia, invece, nel trasferimento di dati verso paesi terzi od organizzazioni internazionali in violazione del Regolamento (UE) 2016/679 [8].

Ancora il **comma IV** è di carattere processuale e disciplina la procedura con la quale il Pubblico Ministero è tenuto ad informare il Garante allorché abbia notizia ovvero quando gli giunga un rapporto dalla Polizia Giudiziaria.

Parimenti, il **comma V** impone un obbligo di denuncia da parte del Garante verso il Pubblico Ministero.

Il **comma VI**, infine, prevede la necessità della sanzione amministrativa pecuniaria irrogata e riscossa dal Garante per ottenere una diminuzione di pena, senza specificarne il *quantum* di riduzione. Col che in assenza di una maggiore precisazione della legge si deve ritenere che la diminuzione sia al massimo di 1/3 [9].

3. Come già anticipato l'elemento del "nocumento", richiesto ai sensi del secondo comma dell'art. 167, è stato oggetto, nel corso degli ultimi anni, di consistenti diatribe giurisprudenziali.

Più nel dettaglio, si sono fronteggiate sul punto due diversi impostazioni.

La prima, sostenuta in passato in via maggioritaria, ne sosteneva la natura di condizione oggettiva di punibilità di tipo intrinseco.

La seconda, al contrario, seguita, peraltro, dalla pronuncia in analisi, ne afferma la valenza in quanto elemento costitutivo del fatto.

Orbene, le ripercussioni scaturenti dall'accoglimento dell'una o dell'altra posizione non sono di poco conto.

Risulta per tale motivo necessario partire da una, seppur breve, analisi degli istituti richiamati.

Partendo dalle condizioni obbiettive di punibilità, queste sono disciplinate all'interno dell'art. 44 c.p. alla luce del quale «quando, per la punibilità del rea-

[7] Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, 22 maggio 2018.

[8] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

[9] V. C. PONTI, *Le fattispecie penali alla luce del novellato codice privacy: il quadro*, in *www.agendadigitale.eu*, 19 dicembre 2018.

to, la legge richiede il verificarsi di una condizione, il colpevole risponde del reato, anche se l'evento, da cui dipende il verificarsi della condizione, non è da lui voluto».

Come risulta facilmente intuibile dal loro nome, trattasi di una peculiare tipologia di condizione imputata oggettivamente all'oggetto agente e a cui l'ordinamento subordina la punibilità di un dato fatto di reato.

La figura *de qua*, più nello specifico, si caratterizza per andare ad inserirsi all'interno di una fattispecie delittuosa già consumata. Ciò, invero, risulta evincibile sin dal dettato normativo, in quanto il già citato art. 44 c.p. fa riferimento alla figura del colpevole [10].

Circa la collocazione delle condizioni obbiettive di punibilità nella struttura del reato, l'orientamento tradizionale è solito qualificarle in quanto elementi estrinsechi della condotta [11].

L'istituto in analisi, infatti, costituisce un avvenimento esterno, aggiuntivo, successivo nonché futuro ed incerto rispetto al fatto di reato, al verificarsi del quale il legislatore subordina l'applicazione della pena.

Orbene, quanto detto rileva per le condizioni c.d. "estrinseche", riconosciute da parte della dottrina come unica tipologie in linea con i principi dell'ordinamento interno quali l'offensività e la colpevolezza [12].

Differisce da queste ultime la *species* c.d. "intriseca", la quale influisce sull'interesse protetto dalla norma nel senso di approfondire una lesione già implicita nella commissione del fatto [13].

Non a caso, infatti, queste vengono sovente sovrapposte agli elementi costitutivi del reato.

Pertanto, nonostante non risulti sempre agevole distinguere le condizioni obbiettive di punibilità dagli elementi costitutivi del fatto di reato, le ripercussioni applicative scaturenti a seconda delle classificazioni normative sono di grande rilievo [14].

---

[10] Cfr. R. Garofoli, *op. cit.*, 2014, p. 542.

[11] Cfr. F. Antolisei, *Manuale di diritto penale parte generale*, Milano, p. 697.

[12] Per la tesi che afferma l'estraneità delle condizioni obbiettive di punibilità al reato cfr. F. Antolisei, *op. cit.*; F. Mantovani, *Diritto penale parte generale*, Padova, 2019, 282; M. Romano, *Commentario sistematico del codice penale*, Roma, 2012, p. 400 ss.; V. N. D'Ascola, *Punti fermi e aspetti problematici delle c.d. condizioni obbiettive di punibilità*, Tip. Iiriti, 1994, p. 652.

[13] In questi termini G. Fiandaca, E. Musco, *Diritto penale parte generale*, Bologna, 2014, p. 775 ss.

[14] Sull'individuazione in concreto dell'esatto *discrimen* sono emerse due tipologie di criteri discretivi. Una prima impostazione, c.d. "diagnostica formale", distingue le figure *de quibus* facendo perno sul mero dato terminologico, ravvisando la sussistenza di una condizione obbiettiva di punibilità ogniqualvolta il legislatore utilizza formule ipotetiche come "qualora" e "nel caso in cui". Si veda sul punto Neppi Modona, *Concezione realistica del reato e condizioni obiettive di*

Basti pensare, a titolo esemplificativo, al *dies a quo* in materia di prescrizione.

Rileva sul punto l'art. 158 c.p., ai sensi del quale nel caso in cui sussista una condizione obbiettiva di punibilità, il *dies a quo* decorre dalla realizzazione della stessa e non dunque da quando reato si consuma [15].

Or dunque, come già poc'anzi anticipato, la giurisprudenza si è a lungo interrogata sul se il nocumento *ex* art. 167 del d.lgs. n. 193/2016, per la persona alla quale i dati illecitamente trattati si riferiscono, sia un elemento costitutivo del reato oppure una condizione oggettiva di punibilità.

La tesi in passato unanimemente seguita qualificava il "nocumento" come condizione obiettiva intrinseca di punibilità [16].

In tal senso si è pronunciata in passato la Cassazione nella sentenza n. 30134/2004, la quale ha precisato che siffatta soluzione rinverrebbe il proprio fondamento nella previsione da parte della norma in esame del dolo specifico di danno.

Quest'ultimo, invero, avrebbe rilevanza solo laddove si dia per presupposta la natura di condizione obiettiva di punibilità del nocumento, poiché, altrimenti, «sarebbe contraddittorio prevedere quale evento del reato uno dei fini perseguiti dal soggetto».

Peraltro, suddetta interpretazione risulterebbe maggiormente conforme alla Carta Costituzionale, in quanto, qualora il nocumento dovesse essere ritenuto

---

punibilità, in *Riv. it. dir. proc. pen.*, 1971. Una diversa, nonché più incisiva, ricostruzione c.d. "sostanziale funzionale", invece, rifugge da impostazioni formalistiche, sostenendo che il *discrimen* tra elementi costitutivi del reato e condizioni obbiettive di punibilità va individuato nel disvalore dell'illecito penale. La fattispecie *ex* art. 44 c.p., infatti, costituisce un evento estraneo alla sfera dell'offesa del reato. Siffatta prospettazione, invero, ne giustificherebbe l'irrilevanza della riferibilità psicologica. V. G. Fiandaca, E. Musco*, op. cit.*, p. 775 ss.

[15] L'art. 158 c.p. dispone che: «Il termine della prescrizione decorre, per il reato consumato, dal giorno della consumazione; per il reato tentato, dal giorno in cui è cessata l'attività del colpevole; per il reato permanente dal giorno in cui è cessata la permanenza. Quando la legge fa dipendere la punibilità del reato dal verificarsi di una condizione, il termine della prescrizione decorre dal giorno in cui la condizione si è verificata. Nondimeno, nei reati punibili a querela, istanza o richiesta, il termine della prescrizione decorre dal giorno del commesso reato. Per i reati previsti dall'articolo 392, comma 1-bis, del codice di procedura penale, se commessi nei confronti di minore, il termine della prescrizione decorre dal compimento del diciottesimo anno di età della persona offesa, salvo che l'azione penale sia stata esercitata precedentemente. In quest'ultimo caso il termine di prescrizione decorre dall'acquisizione della notizia di reato».

[16] Si veda sul punto Cass. pen., Sez. III, 26 marzo 2004, n. 28680, M., in *CED Cass.*, n. 229465 e Cass. pen., Sez. III, 9 luglio 2004, n. 30134, B., in *CED Cass.*, n. 229472; Cass. pen., Sez. III, 17 aprile 2008, n. 16145, A., *in CED Cass.*, n. 239898; Cass. pen., Sez. V, 2 dicembre 2011, n. 44940, C., in *CED Cass.*, n. 251448 nonché Cass. pen., Sez. III, 18 dicembre 2014, n. 7504, P., in *CED Cass.*, n. 259261.

elemento costitutivo del reato, si determinerebbe una notevole riduzione dell'incidenza della tutela penale a causa della difficoltà di reperire l'elemento intenzionale e ciò potrebbe essere indice di una violazione della normativa comunitaria e dei diritti fondamentali garantiti dalla Costituzione [17].

Con maggior impegno esplicativo, trattasi, a detta degli ermellini, di una condizione "intrinseca" di punibilità, che svolgerebbe la sola funzione di circoscrivere la punibilità alle ipotesi in cui la progressione criminosa renda non più tollerabile l'iniziale offesa al bene tutelato e come tale dovrebbe essere in ogni caso sorretta quanto meno dalla colpa.

Un'impostazione diversa, seguita allo stato dalle più recenti pronunce della Corte di Cassazione, qualifica il "nocumento" previsto dall'art. 167 del d.lgs. n. 196/2003 come elemento costitutivo del reato per la sua omogeneità rispetto all'interesse leso e la sua diretta derivazione causale dalla condotta tipica [18].

Ne consegue che esso deve essere previsto e voluto dal *reo* come conseguenza della propria azione.

Le argomentazioni sostenuti da suddetta posizione sono plurime.

In primo luogo l'impostazione *de qua* sottolinea che il nocumento rappresenta l'evento che giustifica la punibilità del reato: risulterebbe, pertanto, anomalo che la condotta di illecito o irregolare trattamento dei dati personali debba essere voluta mentre la conseguenza che ne deriva, che segna, peraltro, il superamento della soglia della penale rilevanza, possa essere imputata anche a titolo di colpa.

In tal senso sarebbe, altresì, anomalo ritenere il dolo necessario per condotte che non rendono attuale l'offesa e non, invece, per il nocumento che rende concreto e attuale il danno e penalmente rilevante la condotta [19].

Peraltro, l'omogeneità del nocumento con l'interesse leso, nonché la sua diretta derivazione causale dalla condotta tipica, indurrebbero a qualificarlo non come elemento estraneo alla fattispecie criminosa ma come elemento costitutivo della stessa.

Da quanto detto deriva che il nocumento, in quanto elementi costitutivo, deve essere previsto e voluto dall'agente come conseguenza della propria azione.

4. Come già anticipato, la Corte, nella pronuncia in analisi, ha risposto alle

---

[17] Cfr. A. Scarcella, *Trattamento illecito dei dati personali: la qualificazione della lesione influisce sulla fattispecie*, in *Contrasti Giurisprudenziali*, 28 gennaio 2016.

[18] V. Sez. III, 5 febbraio 2015, n. 40103 – dep. 6 ottobre 2015, C., in *CED Cass.*, n. 264798.

[19] Cfr. A. Scarcella, *op. cit.*

istanze attoree con una dichiarazione di inammissibilità, giudicando, peraltro, la infondatezza del ricorso di "macroscopica evidenza".

Più nel dettaglio, a detta dei giudici di Piazza Cavour, il ricorrente si è limitato ad opporre alle argomentazioni sviluppate dai giudici del gravame "generiche ed apodittiche considerazioni", riferendosi da un lato ad un non meglio specificato danno non patrimoniale conseguente all'aver "visto diffuso dati afferenti la sfera più intima della persona", dall'altro ad un danno patrimoniale scaturito dall'aver indotto la controparte ad una "transazione al 50% della vertenza giudiziaria per evitare la più che probabile, a tal punto, soccombenza processuale".

Invero, sul punto le osservazioni dedotte dalla Corte sono duplici.

In primo luogo, in riferimento all'avvenuta transazione, la terza sezione, in mancanza di ulteriori specificazioni da parte del ricorrente, lamenta la mancanza di una effettiva correlazione con la lesione rilevata dalla parte.

In secondo luogo, i giudici sottolineano l'impossibilità di poter individuare un effettivo nesso tra la dedotta impossibilità di reinserimento nel mondo del lavoro e la produzione di documentazione medica di tipo psichiatrico prodotto nel corso del giudizio civile ed indirizzata esclusivamente a specifici soggetti ivi coinvolti.

Orbene, prescindendo dagli aspetti prettamente processuali del caso *de quo,* risulta in particolar modo rilevante ai fini di tale analisi soffermarsi sulle argomentazioni giuridiche adottate dai giudici.

In particolare, gli ermellini, avallando le conclusione esperite dalla Corte territoriale, nonostante la produzione della documentazione medica fosse avvenuta ledendo i doveri di correttezza, pertinenza e non eccedenza stabiliti *ex lege* ai fini dell'esercizio del diritto di difesa [20], in quanto ultronea rispetto agli argomenti spesi per negare la sussistenza del credito, alla luce hanno ritenuto insussistente il requisito del nocumento e per tale motivo hanno dichiarato il ricorso inammissibile.

Con maggior impegno esplicativo i giudici, pur senza esplicitamente richiamare il principio di offensività, hanno statuito che la diffusione di dati personali tra specifici individui come cancellieri giudici e avvocati, assoggettati alla luce della carica rivestita, ad un dovere di riservatezza professionale rende la condotta del convenuto non lesiva e pertanto non sanzionabile penalmente.

Risulta, pertanto, facilmente intuibile come la Corte abbia voluto incentrare il proprio *decisum* su una valutazione afferente l'offensività della condotta posta

[20] V. F.P. Luiso, *Istituzioni di diritto processuale civile,* Torino, 2018, 33.

in essere dal *reo,* pur se senza mai farne esplicitamente riferimento all'interno di siffatta pronuncia.

Invero, prescindendo da valutazioni afferenti la mera violazione normativa, il sol fatto che la diffusione di dati sensibilissimi sia avvenuta all'interno di una stretta cerchia di individui, vincolati, alla luce della carica ricoperta, da un generico dovere di riservatezza professionale, rende la condotta non lesiva ed in quanto tale non penalmente sanzionabile [21].

[21] Per un approfondimento sui nuovi aspetti concernenti il principio di offensività, M. Santise, *Coordinate ermeneutiche di diritto penale*, Torino, 2018, p. 147 ss.

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA X, C-486/12, ECLI:EU:C:2013:836

Adrián Palma Ortigosa

Hechos: Un ciudadano solicita a su ayuntamiento una serie de datos personales que este último ostenta respecto del ciudadano, el consistorio accede a la solicitud, entregándole un extracto con dichos datos personales e imponiéndole por los costes de gestión una tasa cuyo importe asciende a 12 €. El ciudadano reclama dicho importe al considerar que está ejerciendo su derecho de acceso a sus datos personales de los que dispone el ayuntamiento, y que por tanto, el ejercicio de dicho derecho no le debería suponer un coste tan excesivo.

Cuestiones claves del asunto:

A) Coste excesivo de la comunicación de datos. Derecho de acceso:

Como premisa, la Directiva 95/46 no exige ni prohíbe a los Estados miembros percibir gastos con ocasión del ejercicio del derecho de acceso a los datos de carácter personal, siempre que el importe de esos gastos no sea excesivo. (FJ 22).

De esta manera, en aquellos casos en los que los Estados miembros hayan previsto el pago de una tasa o importe como contrapartida del ejercicio del derecho de acceso, dicho importe deberá establecer una cuantía que constituya un justo equilibrio entre: (FJ 28)

- Por un lado, el interés de la persona afectada en proteger su vida privada, en especial por medio de su derecho a que se le comuniquen los datos en forma inteligible
- Y por otro lado, el intereses del responsable en relación a la carga que le puede suponer a este último la obligación de comunicar tal información derivada del ejercicio del derecho de acceso por parte del interesado.

Decisión Final: De esta manera, el artículo 12, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que, para garantizar que los gastos percibidos con ocasión del ejercicio del derecho de acceso a los datos de carácter personal

no sean excesivos a efectos de esa disposición, el importe de esos gastos ***no debe exceder el coste de la comunicación*** de dichos datos. (FJ 31). Sin que además, dicha cuantía pueda constituir un obstáculo al ejercicio del derecho de acceso garantizado por la Directiva.(FJ 29)

Artículos implicados del REPD: Art.15.3

Apartado concreto del Temario: 1.5.2

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA IPI, C-473/12, ECLI:EU:C:2013:715

Adrián Palma Ortigosa

Hechos: Un organismo profesional (IPI), a fin de investigar infracciones de la deontología de una profesión regulada**,** contrata los servicios de un detective privado para que este último investigue si determinadas personas que se hacen pasar por agentes inmobiliarios realmente lo son. Se pone en cuestión si la obtención de dicha información que contiene determinados datos personales por parte de estos detectives privados ha vulnerado el contenido de la Directiva 95/46. Concretamente se pretende dilucidar si entre las excepciones que prevé la Directiva a la hora de permitir la obtención de información sin comunicación del interesado, están comprendidas las actuaciones de los detectives privados.

Cuestiones claves del asunto:

A) Concepto de datos. Datos obtenidos por un detective

De entrada, es preciso señalar que unos datos que recaban los detectives privados en relación a unas personas que actúan como agentes inmobiliarios constituyen datos personales a efectos de la Directiva 45/96 dado que afectan a personas físicas identificadas o identificables. Además, su recogida, conservación y transmisión por un organismo regulado como el IPI o por los detectives privados que actúan por cuenta de éste presentan, por consiguiente, el carácter de tratamiento de datos personales en el sentido del Art 2 d) de la mencionada Directiva (FJ 26)

B) Posibilidad de establecer excepciones del deber de informar al interesado establecido en la Directiva

Se parte de la premisa de que, según lo establecido en el Art 13.1 de la Directiva, (artículo que regula las excepciones y limitaciones al derecho a la protección de datos), resultan dos aspectos básicos:

• Los Estados no están obligados a establecer excepciones a ese deber de información de los interesados.

• Pero a su vez, los Estados son libres de establecer distintas medidas legales que en parte limiten tal deber de información del responsable en favor del interesado. De esta manera, del contenido de dicho precepto se extrae que el legislador pretendió dejarles la opción a los EEMM de decidir si – y, en su caso, en relación con qué objetivos – desean adoptar dichos estados las medidas legales para limitar concretamente el alcance de las obligaciones de información del interesado. (FJ 32 y 37)

C) Alcance de dichas excepciones en relación a la figura del detective privado

Por tanto, permitida la posibilidad de que los Estados puedan establecer excepciones al deber de información en favor del responsable de los datos en caso de que no haya existido consentimiento respecto de los interesados. Se analiza ahora sí, la actividad de detective privado que actúa bajo las órdenes de un organismo regulado como el IPI, está comprendida en el ámbito de aplicación de las excepciones establecidas en el artículo 13, apartado 1, letras d) y g), de la Directiva. Así, teniendo en cuenta el tenor literal del Art 13 d), se ha de entender que dado que la profesión de agente inmobiliario constituye una profesión regulada en Bélgica y que el IPI es un organismo profesional encargado de velar por el cumplimiento de la normativa en cuestión, investigando y denunciando las infracciones de dicha normativa. FJ 42. Hay que entender que dicha actividad está comprendida en el ámbito de aplicación de dicha excepción. (FJ 43).

De manera que lo esencial aquí es comprobar si el Estado regulo o no dichas excepciones, así:

- Si un Estado miembro decidió transponer la excepción establecida en el citado artículo 13, apartado 1, letra d), el organismo profesional afectado y los detectives privados que actúan para él pueden invocarla y no están sujetos a la obligación de informar al interesado establecida en los artículos 10 y 11 de la Directiva 95/46. (FJ 45)
- Por el contrario, si el Estado miembro no estableció dicha excepción, los interesados deben ser informados del tratamiento de sus datos personales, según las modalidades y en particular lo contenido en los artículos 10 y 11 de la Directiva. (FJ 46)

Decisión Final: Por tanto, según el TJUE, los Estados miembros pueden establecer que un organismo profesional regulado como el IPI, pueda, solo o con la ayuda de detectives privados, investigar eventuales infracciones de las normas de deontología – incluidas infracciones resultantes de actuaciones de

personas que no cumplieron las normas relativas al acceso a la profesión – al estar cubierto por dicha excepción. (FJ 51)

La actividad de detective privado que actúa para un organismo profesional a fin de investigar infracciones de la deontología de una profesión regulada – en el presente caso, la de agente inmobiliario – está comprendida en el ámbito de aplicación de la excepción establecida en el artículo 13, apartado 1, letra d), de la Directiva 95/46. (FJ 53)

Artículos implicados del REPD: Art 23.1 g) (Excepciones a la obligación de informar), Art 14 , Art 12.

Apartado concreto del Temario: 1.5.7 Excepciones y 1.5.1 Transparencia e información.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA MICHAEL SCHWARZ / STADT BOCHUM, C-291/12, ECLI:EU:C:2013:670

Adrián Palma Ortigosa

Hechos: El Sr. Schwarz solicitó a la Stadt Bochum, esto es, la autoridad encargada de expedir pasaportes, que le expidiera dicho documento, no obstante, este ciudadano se negó a que le tomaran sus huellas dactilares a la hora de expedir tal pasaporte. La Stadt Bochum negó tal solicitud, de manera que el Sr. Schwarz interpuso recurso ante el órgano jurisdiccional correspondiente con objeto de que se ordenara a Stadt Bochum que le expidiese un pasaporte sin tomar sus impresiones dactilares. Este ciudadano entiende que la obligación establecida por el Reglamento 2252/2004 relativa a la toma de huellas dactilares en caso de solicitud de un pasaporte es contraria al derecho a la protección de datos personales plasmado en el Art 8 CDFUE.

Cuestiones claves del asunto:

A) Dato personal y tratamiento de datos. Huella dactilar:

Las impresiones dactilares han de considerarse datos personales en la medida que estas contienen objetivamente información única sobre personas físicas y permiten su identificación precisa. (FJ 27). Además, se produce un tratamiento de datos en la medida que las autoridades nacionales toman las impresiones dactilares de los interesados y además, las mismas son conservadas en el dispositivo de almacenamiento integrado en el pasaporte. (FJ 29). De esta manera, la exigencia de tomar las impresiones dactilares es una injerencia al derecho a la protección de datos. (FJ 30). Se ha de valorar por tanto si dicha injerencia está o no justificada.

B) Vulneración o no del derecho a la protección de datos:

Pues bien, en virtud del Art 8.2 CDFUE el tratamiento de datos solo puede basarse en el consentimiento del interesado o en virtud de otro fundamento legítimo (FJ 31). Así, en el caso analizado hay que excluir el consentimiento del

interesado como mecanismo que legitima el tratamiento ya que el Reglamento que se analiza impone a los interesados la obligación de plasmar sus huellas digitales en el pasaporte. (FJ 32). Ello lleva a analizar en su caso cual es el interés legítimo que justifica tal restricción de este derecho. Para ello, y conforme al Art 52.1 CDFUE, se ha de analiza si tal limitación está establecida por ley, respeta el contenido esencial, observa el principio de proporcionalidad y además dicha limitación es necesaria y responde a un objetivo de interés general.

Pues bien, en primer lugar, tal limitación está prevista por ley (Reglamento) (FJ 35), en segundo lugar, se analizan los objetivos que subyacen en dicha limitación, así, dichos objetivos son:

- Prevención de la falsificación de pasaportes.
- Evitar el uso fraudulento del pasaporte, esto es, su uso por personas que no sean su legítimo titular, (FJ 36), impidiendo con ello la entrada ilegal de personas en el territorio de la Unión. (FJ 37).

Por lo que se refiere a la proporcionalidad de la medida en razón del objetivo que se persigue, el TJUE considera que dicha medida es proporcional ya que la impresión dactilar de huellas es un medio idóneo para alcanzar el objetivo de prevenir la falsificación de pasaportes (FJ 41). Además, tal medida reviste el carácter necesario de ese tratamiento, ya que como tal no es una medida especialmente agresiva. (FJ 48).Y a día de hoy no existen otras alternativas menos agresivas y más desarrolladas. (FJ 51 y 52). Por último, y por lo que se refiere al uso que en su caso puedan realizar las autoridades a dichos datos que obtienen, el TJUE no considera que se haya demostrado que exista un uso fraudulento. (FJ 53 y ss)

Decisión Final: La obligación de impresión de huellas dactilares como condicionante de obtención de emisión del pasaporte es una limitación al derecho a la protección de datos que está justificada por los objetivos que se persigue con dicha media. (FJ 64)

Artículos implicados del REPD: Art.4.1, 4.2. (Definición de datos y de tratamiento)

Apartado concreto del Temario: 1.2.2.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA WORTEN Y ACT, C-342/12, ECLI:EU:C:2013:355

Adrián Palma Ortigosa

Hechos: Tras unas actuaciones llevadas a cabo por la Inspección de Trabajo portuguesa, esta última decide imponer a la empresa supervisada una sanción administrativa al considerar que dicha empresa debería de haber concedido en el momento solicitado por la Inspección de Trabajo una serie de datos referidos a los horarios de los trabajadores de entrada y salida. Esta sanción fue recurrida por la empresa, el tribunal que conoció del asunto decidió plantear cuestión prejudicial ante el TJUE para valorar si una norma que obliga a otorgar el registro de los horarios de los trabajadores en el instante que lo solicita la autoridad laboral es conforme o no a la Directiva 96/45. Concretamente en lo referido a la licitud del tratamiento. Hay que señalar que, si bien el tribunal nacional no plantea correctamente las cuestiones prejudiciales, el TJUE las reorienta.

Cuestiones claves del asunto.

A) Concepto de dato personal y tratamiento:

Los datos que figuran en un registro del tiempo de trabajo donde se incluyen los períodos de trabajo diario y a los períodos de descanso de cada trabajador, constituyen *datos personales* en el sentido del artículo 2, letra a), de la Directiva 95/46, dado que se trata de información sobre una persona física identificada o identificable. (FJ 19). A su vez, la recogida, registro, organización, conservación, consulta y utilización de tales datos por el empleador, así como su transmisión por este último en favor de las autoridades nacionales competentes en materia de supervisión de las condiciones de trabajo, revisten, el carácter de *tratamiento de datos personales*. (FJ 20)

B) Sobre La licitud del registro de horarios

El TJUE considera que el tratamiento de datos personales analizado, esto es, el registro de horarios, es totalmente lícito, y ello es así porque dicho

tratamiento se recaba con el fin de cumplir con la normativa sobre las condiciones de trabajo, resultando ser dicho tratamiento necesario tanto para el cumplimiento de las obligaciones jurídicas a las que está sujeto el empleador en esta materia , como para la ejecución de las misiones de control confiadas a la Inspección de Trabajo en la supervisión de las condiciones de trabajo. (FJ 35 y 34).

C) Obligación de proporcionar a la autoridad el acceso inmediato al registro

Por último, el TJUE considera que la obligación de proporcionar a la inspección de trabajo el registro inmediato se desprende del Art 7 de la Directiva, ello es así debido a que esta obligación puede resultar necesaria, en los términos descritos en dicho precepto, para contribuir a una aplicación más eficaz de la normativa en materia de condiciones de trabajo (FJ 37). Evitándose con ello además, que el empleador pueda alterar los datos del registro entre el momento de la inspección y aquel en que finalmente se facilitan los datos. (FJ 41)

Decisión Final: El TJUE señala por tanto que, los artículos referidos a los principios del tratamiento Art 6.1 b) y c), así como a la licitud de dicho tratamiento (Art 7c y e), no se oponen a una normativa nacional como la controvertida en el litigio principal que impone al empleador la obligación de poner a disposición de la autoridad nacional competente el registro del tiempo de trabajo con el fin de supervisar las condiciones de trabajo.

Debiendo permitirse la consulta inmediata de dicho registro, siempre que esta obligación ***sea necesaria*** para el ejercicio por esta autoridad de la misión de supervisión que le incumbe en relación con la normativa sobre condiciones de trabajo y, especialmente, de la relativa al tiempo de trabajo.

Artículos implicados del REPD: Art 6.e) (licitud del tratamiento), Art 88. (Tratamiento en el ámbito laboral. Art 4.1) y 2) Concepto de dato y de tratamiento

Apartado concreto del Temario: 1.3.2, 1.2.2

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA COMISIÓN EUROPEA/AUSTRIA, C-614/10, ECLI:EU:C:2012:631

Adrián Palma Ortigosa

Hechos: La Comisión y el Supervisor Europeo de Protección de Datos consideran que Austria no ha transpuesto correctamente la Directiva sobre protección de datos al establecer determinadas previsiones normativas que dejan en entredicho la independencia que ha de ostentar la autoridad de control de protección de datos austriaca (DSK). El gobierno austriaco se opone a ello.

Cuestiones claves del asunto:

A) Independencia de la autoridad de control:

Para el TJUE, la creación en cada uno de los Estados miembros de autoridades de control independientes constituye un elemento esencial del respeto al derecho a la protección de los datos personales (FJ 37). Art 28 Directiva y 8.3 CDFUE. (FJ 36). Esta independencia exige que dichas autoridades ejerzan sus funciones sin ningún tipo de influencia externa. (FJ 41). Excluyéndose no solo la influencia directa, en forma de instrucciones, sino también, toda forma de influencia indirecta que pueda orientar las decisiones de la autoridad de control (FJ 43). En el caso analizado, se ha acreditado que existe una relación de servicio entre la autoridad de control de protección de datos y la autoridad federal, lo cual permite al superior jerárquico (autoridad federal) de dicha autoridad de control controlar sus actividades (FJ 48 y 50), lo que podría llevar a la autoridad de control a adoptar una actitud de «obediencia anticipada» que busque posibles promociones futuras. (FJ 51 Y 52). Por otro lado, esta independencia se ve también menoscabada en relación al personal que trabaja para la autoridad de control (secretaría), ya que son funcionarios federales de la autoridad pública correspondiente. (FJ 61).

Es decir, estos hechos ponen en entredicho la necesaria independencia que ha de ostentar la autoridad de control de protección de datos austriaca.

Decisión Final: Por tanto, Austria ha incumplido las obligaciones que le incumben en virtud del artículo 28.1.párrafo 2 de la Directiva 95/46, al no haber adoptado todas las medidas necesarias que la legislación europea exige relativas al requisito de independencia del que ha de gozar toda autoridad de control y, más concretamente, al haber establecido un marco normativo en virtud del cual:

- el administrador de la DSK (autoridad de control de protección de datos) es un funcionario federal sometido a supervisión jerárquica;
- la secretaría de la DSK está integrada en la Cancillería federal, y
- el Canciller federal tiene un derecho incondicional a informarse de todos los aspectos de la gestión de la DSK

Exigencias normativas que denotan esa falta de independencia que la Directiva 95/46 impone a los EEMM.

Artículos implicados del REPD: Considerando 117, 118, Art 51, 52, 53 y 54

Apartado concreto del Temario: 1.10.1

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA COMISIÓN/ALEMANIA, C-518/07, ECLI:EU:C:2010:125

Adrián Palma Ortigosa

Abstract:

La Comisión y el Supervisor Europeo de Protección de Datos consideran que Alemania está incumpliendo el Art 28.1 de la Directiva 95/46 al no cumplir con el requisito de independencia que ha de acompañar a toda Autoridad de Control de protección de datos. En este sentido, la normativa alemana prevé el sometimiento de las Autoridades de control a la tutela del Estado.

Cuestiones claves del asunto:

A) Independencia de la Autoridad de Control:

El TJUE razona que la independencia de la autoridad de control exigida por la Directiva garantiza a dicha autoridad la posibilidad de actuar con plena libertad y a resguardo de cualquier tipo de instrucciones o presiones. (FJ 18), implicando con ello una facultad de decisión exenta de toda influencia externa a la autoridad de control, ya sea directa o indirecta (FJ 19). En este sentido, para preservar de forma eficaz y fiable el respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales, se exige que dicha autoridad actúe con objetividad e imparcialidad. (FJ 25).

En el caso objeto de estudio, la previsión legal por la cual el estado alemán a través de sus administraciones tutela las labores de las autoridades de control, permiten a dichas administraciones influir directa o indirectamente en las decisiones de las autoridades de control o, incluso, anular o sustituir estas decisiones. (FJ 32), sin que además, se puede descartar que las autoridades de tutela, que forman parte de la Administración general y, por tanto, están sometidas al Gobierno de su respectivo Land , no sean capaces de actuar de forma objetiva al interpretar y aplicar la normativa en materia de tratamiento de datos personales.(FJ 34) .

De esta manera, la mera posibilidad de que las autoridades de tutela puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de éstas, ya que, podría darse en tal caso una «obediencia anticipada» de las autoridades de control a la vista de la práctica decisoria de la autoridad de tutela. (FJ 36)

Decisión Final: Habida cuenta de las consideraciones anteriores, ha de declararse que la tutela del Estado ejercida sobre las autoridades de control alemanas competentes para vigilar el tratamiento de datos personales en el sector no público no es compatible con la exigencia de independencia. (FJ 37).

Artículos implicados del REPD: Considerando 117, 118, Art 51, 52, 53 y 54

Apartado concreto del Temario: 1.10.1

SENTENCIAS DEL TRIBUNAL SUPREMO. (SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO)

STS 3896/2014 - ECLI: ES:TS:2014:3896

Adrián Palma Ortigosa

Hechos: Promusicae (entidad privada) solicitó a la AEPD al amparo del artículo 5.5 de la LOPD, la exención del deber de informar a los usuarios de redes peer to peer (P2P) del tratamiento de datos que dicha entidad privada pretendía llevar a cabo para el ejercicio de defensa de los derechos de propiedad intelectual de los productores y editores de fonogramas y videos musicales. Esencialmente, Promusicae pretendía recabar las direcciones IP de los usuarios que accedían a esas redes P2P y se descargaban determinados contenidos digitales para posteriormente poner a disposición de las autoridades correspondientes dichas direcciones IP de cara a emprender acciones judiciales contras las personas que se descargaban y compartían tales contenidos.

Cuestiones claves del asunto:

A) Concepto de datos personal. IP:

El TS considera que las direcciones IP son datos personales en el sentido del Art 3 LOPD ya que contienen información concerniente a personas físicas "identificadas o identificables". En este sentido, el hecho de que la entidad PROMUSICAE indique que no tiene al alcance de su mano la identificación del titular de los datos por medios y plazos razonables, no es obstáculo para concluir tal consideración de dato personales, ello es así porque a partir de una dirección IP, puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado dichas direcciones IP. Todo ello teniendo en cuenta que, tanto el Art 3 a) de la LOPD como el 2 a) de la Directiva 95/46 vienen a indicar que "*se considerará identificable toda persona cuya identidad pueda determinarse, directa* ***o indirectamente***..." (FJ 4o)

B) Exención del deber de informar al interesado por medio de la aplicación del Art 5.5 LOPD

Sentada la premisa por la cual, una dirección IP es un dato personal, el TS pasa a analizar si nos encontramos dentro de uno de los supuestos contenidos en el Art 5.5 LOPD que permite eximir al responsable del tratamiento el deber de informar a los interesados de que sus datos están siendo tratados. Así, este precepto exceptúa tal deber de información para:

- Cuando una ley expresamente lo prevea.
- Cuando el tratamiento de datos personales obedezca a fines históricos, estadísticos o científicos.
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados.

En este sentido, Promusicae aludió a este último mecanismo, indicando que el deber de información en estos casos le supondría un esfuerzo desproporcionado. En respuesta a esta alegación, tanto la AEPD, como la Audiencia Nacional que fue el órgano jurisdiccional que en un primer momento conoció del asunto, consideraron que no se daba tal motivo alegado por Promusicae. Pues bien, el TS, tras hacer alusión a todo ello, llega a la misma conclusión que los órganos anteriores entendiendo que Promusicae no ha acreditado suficientemente las circunstancias establecidas en el artículo 5.5 LOPD que le habilitan para aplicar la exención del deber de informar. (FJ 5o)

C) Consentimiento tácito:

Seguidamente, el TS pasa a analizar si en el caso analizado ha existido consentimiento tácito por parte de los interesados para el tratamiento de datos que pretende por el mero hecho de que dichos usuarios accedan a dicha red P2P.

Así, el TS llega a la conclusión de no existe consentimiento a los efectos de la normativa de protección de datos, ya que, si bien el artículo 6 LOPD permite el consentimiento tácito, este también requiere que sea inequívoco, no presumiéndose tal característica para los casos en los que una persona se conecta a una red P2P en la que su dirección IP es pública. Por consiguiente, el hecho de que un usuario de red P2P conozca que su dirección IP es visible y puede ser conocida, no significa que acepte de forma inequívoca su uso y tratamiento por terceros, ni que consienta de forma específica el tratamiento de sus datos que pretende la parte recurrente, ya que no se puede olvidar que, a la hora de valorar si existe un consentimiento tácito por parte del interesado para su tratamiento se han de tener en cuenta la finalidad de los actos de los que se deduce esa voluntad. En este caso, la finalidad por la cual, la dirección IP es pública, obedece simplemente al hecho de que ello es necesario para poder operar en las redes P2P, de manera que no resulta razonable deducir que con

ello a su vez se esté prestando por parte del interesado consentimiento para el tratamiento automatizado de sus datos en favor de un tercero.

D) No exigencia del consentimiento cuando la ley así prevea.

El TS analiza si existe alguna norma que permita a Promusicae tratar los datos de los interesados sin el consentimiento de estos conforme al Art 6.1 in fine LOPD. Para ello, Promusicae alude a varias normas en materia de propiedad intelectual, así como al propio derecho a la tutela judicial efectiva (Art 24) para apoyar su argumento por el cual, dichas normas habilitarían a esta entidad privada a tratar los datos sin necesidad del consentimiento de los interesados. Sin embargo, el TS viene a indicar que ninguna de estas normas señala expresamente tal excepción a la exigencia de consentimiento por parte de los interesados, ya que, toda normativa que excepcione el consentimiento del interesado a la hora de tratar sus datos ha de ser precisa y señalar expresamente tal situación. (FJ 7o).

E) Derecho a la protección de datos vs propiedad intelectual. Licitud del tratamiento

Se valora ahora el posible tratamiento lícito que ostenta Promusicae para tratar los datos sin el consentimiento del interesado conforme al Art 6.2 LOPD y el Art 7.f) Directiva 95/46. Así, lo que Promusicae plantea en este caso al TS es el hecho de que pondere y valore, si el tratamiento de datos que pretende realizar Promusicae se ha de considerar lícito conforme a lo establecido en el Art 7 f) Directiva 95/46 y Art 6.2 LOPD. Debiendo valorar el TS dos aspectos para que en su caso dicho tratamiento sea lícito:

1. Que dicho tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable (En este caso Promusicae)
2. Que dicho interés legítimo prevalezca respecto de los derechos y libertades fundamentales del interesado.

Pues bien, en relación al primer requisito, para el TS, Promusicae no ha acreditado suficientemente la concurrencia de la necesidad de acudir al tratamiento de datos en cuestión. En este sentido, el TS tiene en cuenta el hecho de que Promusicae en ningún momento ha ofrecido indicación alguna, siquiera aproximada, sobre el número de interesados cuyos datos personales pueden ser objeto del tratamiento exento de su autorización, además, el TS también valora el hecho de que dicho tratamiento será realizado por una empresa danesa domiciliada en Copenague. Empresa esta última encargada de realizar la prestación de servicios por la que tratarían dichas direcciones IP junto con otros datos de los interesados.

Decisión Final: - El TS considera que una dirección IP es un dato de carácter personal en el sentido del artículo 3.a) LOPD y, como tales, dichos datos se encuentran protegidos por la normativa en materia de protección de datos.

– El hecho de que unos usuarios accedan a una red P2P donde su dirección IP es pública no ha de entenderse como el otorgamiento de consentimiento tácito del tratamiento de sus datos personales por parte de terceros.

– El tratamiento de datos que pretende llevar a cabo Promusicae no puede entenderse legitimo conforme a las exigencias del Art 6.2 LOPD y Art 7 f) Directiva 95/46, ya que dicha entidad privada no ha acreditado suficientemente la estricta necesidad para la finalidad legítimamente perseguida. (FJ 8o in fine)

Artículos implicados del REPD: Art 4.1, Art 7, Art 6.1 f)

Apartado concreto del Temario: 1.2.2, 1.4.3 y 1.3.2

SENTENCIA TRIBUNAL SUPREMO. (SALA SOCIAL 13 DE MAYO DE 2014)

ECLI:ES:TS:2014:2618

María Bocio Jaramillo

Cuestiones de hecho: Nos encontramos ante un supuesto de despido de una trabajadora de supermercado debido a las conductas de sustracción de la recaudación de la caja de este. La misma, al llevar a cabo dichas conductas, fue captada por cámaras de videovigilancia cuya instalación no fue consentida ni informada de manera previa y tampoco fue informado que dichas cámaras tenían como finalidad el control de la actividad laboral. Por ello, se plantea si existe o no vulneración del derecho a la protección de datos personales recogido en el artículo 18.4 CE. En las sentencias de instancias anteriores, el despido se consideró nulo, procediendo la representante del supermercado a recurrir en casación ante el TS.

Cuestiones claves y fundamentos jurídicos:

1. Confrontación con doctrina establecida con anterioridad por el TS basada en la argumentación sostenida por el TC:

Con respecto a la STC 186/2000 de 10 de julio, el TS entiende que nos encontramos ante supuestos distintos, debido a que, en el caso que se presentó ante el TC y que le sirve de fundamento a dicha sentencia, el uso de las cámaras se estableció específicamente para controlar la actividad de la trabajadora ante las sospechas de irregularidades que se estaban produciendo. Por ello, se entendió que la medida era adecuada y proporcionada para alcanzar la finalidad a la que se atendió. Consideró el tribunal que: "era una medida justificada (ya que existían razonables de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y

equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 C.E., "añadiendo que" la intimidad del recurrente no resulta agredida por el mero hecho de filmar cómo desempeñaba las tareas encomendadas en su puesto de trabajo, pues esa medida no resulta arbitraria ni caprichosa, ni se pretendía con la misma divulgar su conducta, sino que se trataba de obtener un conocimiento de cuál era su comportamiento laboral, pretensión justificada por la circunstancia de haberse detectado irregularidades en la actuación profesional del trabajador, constitutivas de transgresión a la buena fe contractual" (FJo2).

2. Derecho de información y consentimiento:

Se considera probado que la información proporcionada determinó que las cámaras de video eran para un sistema de control del cliente y no de la relación laboral, inclusive, previa interpelación de los trabajadores. No se informó, en ningún momento, del alcance del tratamiento de datos consistente en: casos en que pueden ser examinadas las imágenes, duración, posibilidad de imponer sanciones por lo recogido en las mismas.

Por lo anterior, no se llevó a cabo una información previa, clara, e inequívoca de la finalidad de control. Además, el tribunal considera que el mero hecho de la instalación y conocimiento de las mismas no es válido para entender la finalidad del control laboral, máxime cuando dicho consentimiento fue negado por los trabajadores, tal y como queda probado (FJ o7).

Valoración final: se desestima el recurso interpuesto por la empresa al no haberse cumplido de manera adecuada el deber de información referente al tratamiento de datos, en este caso de imágenes (FJo7).

Voto particular: dentro de sus argumentos es digno de destacar, el referente a que el conocimiento de la instalación de las cámaras, sabiendo que las mismas grababan el pasillo donde se encontraban los clientes y también las cajas, es suficiente para deducir implícitamente dicha finalidad de control de la actividad laboral. Considera que la grabación de las cajas es una medida proporcionada, necesaria e idónea para evitar sustracciones y no para otros fines distintos a este. Para finalizar desarrolla un argumento más que interesante al disponer que: "Dejando a un lado el hecho de si hubo o no un tratamiento de datos ilícito por la simple captura de unas imágenes un día, el problema es ¿Qué pasa con los

hallazgos causales? ¿Qué sucede si la cámara visiona en la cola de la caja un homicidio, un acoso sexual u otro delito cometido por un empleado? ¿Estaremos ante una prueba ilícita y el acosador u homicida serán absueltos?. La respuesta no puede ser positiva, la protección de los derechos fundamentales no puede ir más allá de lo razonable y el derecho a la intimidad y a la protección de datos no puede proteger a los autores de estos hechos ilícitos cuando su acción ha sido advertida por un control causal, hecho por cámaras a la vista cuya existencia es conocida por el autor, aunque no se le haya advertido de que se podrán utilizar en su contra".

Artículos del repd: Artículos 7, 13, 23, 88 y Considerandos 42, 43 y 50.2.

Apartado concreto del temario: 1.12.5 Videovigilancia.

SENTENCIAS DEL TRIBUNAL SUPREMO.
(SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO)
STS 7583/2011 - ECLI: ES:TS:2011:7583

Adrián Palma Ortigosa

Hecos: Una ciudadana solicitó a la Prelatura del Opus Dei que, en un plazo de diez días, le remitiera certificación en la que se hiciera constar por dicha entidad la cancelación de sus datos personales contenidos en los archivos del Opus Dei. Dicha entidad denegó tal solicitud, señalando que los únicos datos referidos a dicha ciudadana son hechos históricos, realizados voluntariamente y que no podía anularse.

Ante tal situación, esta ciudadana presentó reclamación ante la AEPD, esta última instó al Opus Dei a la cancelación de tales datos. Como consecuencia de ello, el Opus Dei recurre ante la AN la decisión de la AEPD, este tribunal ratifica lo señalado por la AEPD, por lo que dicha entidad religiosa plantea recurso de casación ante el TS.

Cuestiones claves del asunto:

A) Derecho a la libertad religiosa vs Protección de datos. Inviolabilidad de los registros.

En el primer motivo, el TS analiza el alcance del Art 1.6 del Acuerdo entre el Estado Español y la Santa Sede sobre Asuntos Jurídicos. Así, conviene indicar que el Art 1.6 del mencionado acuerdo viene referido a la ***inviolabilidad*** de los archivos y registros pertenecientes a las instituciones católicas correspondientes. Pues bien, según el TS:

- Conforme a la jurisprudencia del TEDH, este precepto ha de interpretarse de acuerdo con la práctica internacional en materia de inmunidades y privilegios de los agentes extranjeros, así como de sus bienes, documentos y archivos, sin que dichas inmunidades puedan anular la dimensión sustantiva de los derecho fundamentales de la persona.
- Además, se ha de tener en cuenta que dicho artículo no puede tener un alcance absoluto cuando el beneficiario de dicho precepto no sea un Estado o una Organización Internacional, sino como ocurre en este caso, una Entidad situada en España, esto es, el Opus Dei.

Es decir, la inviolabilidad de los documentos mencionados en dicho Art 1.6 no es absoluta, y más, cuando dicha inviolabilidad se pretende hacer valer frente a los particulares. En este sentido, TS viene a desmontar el argumento del Opus Dei referido a que dicha inviolabilidad no la invoca frente a un particular, sino que la realiza respecto a una entidad pública, en este caso la AEPD. Así, el TS deniega tal argumento al señalar que resulta evidente que la AEPD actúa en ejercicio de sus funciones de tutela en materia de protección de datos que le encomienda la LOPD, tutela que se ejercita tras la solicitud de la ciudadana que solicita la cancelación de los datos relativos a su persona, que fue denegada por el Opus Dei. (FJ 3o)

B) Concepto de Fichero. Inscripción y cancelación en la Prelatura.

En segundo lugar, se valora si los datos personales que obran en poder de la Prelatura del Opus Dei de la interesada, esto es, el nombre y apellidos, fechas de incorporación y baja en la Prelatura, están incorporados a un fichero o en su caso sometidos a un tratamiento conforme a la normativa en protección de datos.

Así, para el TS, no existe duda que nos encontramos ante un fichero en el amplio sentido de la LOPD y Directiva 95/46 /CE, pues la información que se recoge:

- Está constituida por datos personales, especialmente protegidos por afectar a las creencias religiosas, y
- Dichos datos están suficientemente organizados, habiendo sido localizados fácilmente por la Entidad religiosa.

C) Cancelación de los datos

En relación a la cancelación de los datos, el Opus Dei viene a indicar que, corresponde al interesado probar que los datos que trata dicha entidad han dejado de ser necesarios para los fines para los que fueron recabados tales datos. (Art 4.5 LOPD)

Sin embargo, el TS vuelve a desmentir tal postura al indicar que la interpretación que realiza el Opus Dei sobre el artículo 4.5 LOPD es errónea. En este sentido, este precepto no obliga ni al interesado ni al responsable a determinar cuando los datos han dejado de ser necesarios, sino que la necesidad del mantenimiento o en su caso la cancelación de los datos ha de relacionarse estrictamente con la finalidad para la cual los datos fueron recogidos. Así, en el caso analizado, los datos dejaron de ser necesarios para la finalidad que justificó su tratamiento en el momento que la persona afectada dejo de pertenecer al Opus Dei, además, se ha de tener en cuenta que dicha entidad religiosa no ha acreditado una finalidad de conservación de los datos merecedora de mayor protección. (FJ 5o)

Decisión Final: --Los archivos, documentos, etc. a los que se refiere el Art 1.6 del Acuerdo entre el Estado Español y la Santa Sede sobre Asuntos Jurídicos son susceptibles de someterse a la normativa en materia de protección de datos, ya que la inviolabilidad predicada por dicho precepto respecto a tales documentos no es absoluta, en especial, frente a particulares.

– Los datos personales referidos a la inscripción y cancelación de un interesado que obran en poder del Opus Dei están incorporados a un fichero, ya que están suficientemente organizados.

– A la hora de valorar si los datos han dejado de ser necesarios o pertinentes de cara a ejercer el derecho de cancelación, se habrá de tener en cuenta la finalidad para la que fueron recogidos dichos datos.

Artículos implicados del REPD: Art 17.1, a) , Art 4.6), Art.9.1, Art 91.

Apartado concreto del Temario: 1.5.2, 1.2.2, 1.4.4.

SENTENCIAS DEL TRIBUNAL SUPREMO. (SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO

STS.CA N.O 6410- 2000 DE 15-12-2004

Adrián Palma Ortigosa

Hechos: Un ciudadano recibe determinado contenido publicitario proveniente de distintas empresas a las que no ha cedido sus datos personales. Estas empresas han recibido dichos datos de otra sociedad (Publienvío). Los datos que aparecen en dicho envío publicitario son datos que parecen provenir del padrón municipal o del censo electoral. La sociedad (Publienvío) niega haber obtenido dichos datos personales del padrón municipal, indicando que dicha información fue obtenida gracias a otra sociedad de la cual se desconoce cómo recabo tales datos.

Cuestiones claves del asunto:

A) Procedencia de los datos:

Para el TS queda ratificado que la obtención de los datos se produjo del padrón municipal o del censo electoral por parte de Publienvío, ya que los envíos publicitarios que recibe este ciudadano indican una serie de datos personales que en parte son erróneos, reproduciéndose de forma similar dichos errores en el padrón municipal y en el censo electoral respecto de ese ciudadano. (FJ 2o Y 3 o)

B) Legitimación del tratamiento:

Para el TS el tratamiento de datos que realiza la mencionada sociedad no cumple las exigencias legales, así:

• Por un lado, no cumple con las exigencias de la LORTA, ya que, el tratamiento de datos de fichero privado obtenidos de fuentes de titularidad pública como el censo electoral, requiere del consentimiento del interesado.

• Por otro lado, el tratamiento llevado a cabo por Publienvío tampoco cumple con las exigencias legales de la Directiva 95/46 sobre protección de datos, ya que, a ante la ausencia consentimiento como base legal del tratamiento (como ocurre en este caso), el tratamiento de datos solo podría ser legítimo si conforme

al Art 7 f) de dicha directiva, el interés legítimo de la sociedad prevaleciera respecto de los derechos y las libertades de los interesados. En este caso en concreto, el interés de las empresas dedicadas a la publicidad o a la venta a distancia no prevalece respecto del interesado. (FJ 4o)

Decisión Final: Publienvío ha incumplido la legislación española y la Directiva 95/46 al tratar los datos personales del interesado sin el consentimiento de este y sin estar amparado en ninguna otra base legal que en su caso pudiera justificar el tratamiento de datos por parte de dicha empresa.

Artículos implicados del REPD: Art 6.1 f), Art 14.2 f)

Apartado concreto del Temario: 1.3.2 y 1.5.1

AUDIENCIA NACIONAL SALA CONTENCIOSO ADMINISTRATIVO DE 28 DE SEPTIEMBRE DE 2001

ECLI: ES:AN:2001:5463

María Bocio Jaramillo

Hechos: En el presente caso se interpone recurso contra la resolución de la Agencia Estatal de Protección de Datos, que había desestimado previamente un recurso de reposición contra una resolución que impuso una multa de 50.000.000 ptas, a "Servicios Jurídicos Alaveses S.A"por infracción del artículo 7.2 LOPD, conllevando una sanción de carácter grave del artículo 43.4.c LOPD. Los hechos tuvieron lugar cuando D. Javier, director del Viceconsejo de Seguridad del Gobierno Vasco, recibe una publicidad, en su lugar de trabajo, referente a un Hotel que le invitaba a una fiesta. En el sobre se hacía contar: nombre y apellidos, dirección y las siglas del PNV. La propietaria del hotel es la responsable de un fichero denominado "Mailing98MDB" y "Mailing.MDB", en los mismos aparecen: su nombre, apellidos, cargo, institución, domicilio laboral. El titular de los datos impugna que dicho fichero contenga informaciones como la relativa a su orientación política, cuestión a la que se opone en el recurso el responsable del fichero, y al mismo tiempo propietaria del hotel, ya que considera que son datos notorios y públicos que constan en la guía de comunicación del gobierno vasco.

1. El consentimiento y las categorías especiales de datos.

La cuestión a tratar y destacar del caso es si los datos de carácter personal, como es por ejemplo la orientación política, al ser de carácter notorio y general deben necesitar del previo consentimiento para incorporarlos a un fichero o no. La Audiencia Nacional considera en su fundamento jurídico 4o que la exigencia del consentimiento previo al tratamiento requiere especial exigencia cuando nos encontramos ante datos referentes a ideología, religión, creencias u otros regulados en el artículo 7.2 LOPD. Con respecto a ellos, se exige un consentimiento expreso y por escrito. Además, entiende que no puede ampararse en la

existencia de que el dato en cuestión sea notorio para no exigir el previo consentimiento.

Considera por otro lado que: "La solución contraria propugnada por la recurrente mediante la identificación de la intimidad y con la protección de los datos, excluyendo de la protección de este último los datos públicos u notorios, conduciría a establecer peligrosas excepciones, a la tutela de los derechos fundamentales, carentes de apoyo constitucional y legal. Además, permitiría, v. gr., tratar de forma automatizada sin consentimiento del afectado, los datos referentes al origen racial de la persona, en los casos que afecta al color de la piel cuyo carácter es notorio, y sin embargo su protección también se intensifica en el artículo 7.3 la Ley Orgánica 5/1992" (FJ 2o).

2. Valoraciòn final.

Se requiere el consentimiento para tratar datos de carácter personal y especialmente aquellos del artículo 7.2 LOPD. EL carácter notorio y público de estos no exime de dicha condición (FJ 2o).

Artículos del REPD: Artículos 6,7 y 9.

Apartado del Temario: 1.4.1 El consentimiento: otorgamiento y revocación, 1.4.4 Categorías especiales de datos.

SECTION III: USE CASES

Challenge Title: Privacy by Design and by Default and Data Protection Impact Assessment (DPIA)	
Use Case Author	Davide Borelli, Lucilla Gatt, Suor Orsola Benincasa University of Naples
Topic	Pharmaceutical
Overview	Get Well Soon' is a leading pharmaceutical company co-headquartered in Italy and the United Kingdom. Amongst others, 'Get Well Soon' focuses on developing smart medical devices many of which can be remotely managed via ad hoc mobile apps. The Head of IT, Davide, is currently developing a new mobile app which links to a smart tooth-brush: any data collected via the use of such device is then processed in the backend and shown to users in an intelligible form. Davide has recently completed his mandatory GDPR training. Having learnt that by law privacy shall be baked into any project development lifecycle from the outset, he is now concerned that his new app, as well as any other app developed by his team is not fully compliant with the applicable data protection legislations. As such, he immediately contacts the Global Privacy Team of 'Get Well Soon' seeking for advice.
1. Engage	
Big idea	Privacy by Design and by Default and Data Protection Impact Assess-ment (DPIA)
Essential Question	What does 'Privacy by Design and by Default' mean in practice? How should it be implemented within an existing Project Management Methodology (PMM) and System Development Life Cycle (SDLC)? How would you spread accountability throughout the business?
Initial resources	1. A brief illustration of the 'Get Well Soon' company structure, and 2. A brief PMM process 3. A brief SDLC process

Guiding Questions	Acting as newly appointed Global Privacy Offices, the Students should try to design a privacy governance model and update the existing SDLC and PMM to bake-in privacy from the very outset. • What does 'Privacy by Design and by Default' means in theory? And in practice? • How would you organise the overall privacy structure at a central and local level? How would you raise awareness (and accountability) throughout the business? • How would you assess potential privacy risks? How would you create momentum for a wider and shared privacy accountability? How would promote a smoother change management process?
Reflections	Once the exercise is completed, the Students will be encouraged to reflect on the many meanings and applications of 'Privacy by Design and by Default' and its ontological mutability. The Students will also be encouraged to think about how a similar scenario could be tackled more effectively in future and to record any individual reflections on the exercise.
Other notes	
2. Investigate	
Activity Description	Each Student is required to map out a process of investigation for answering the questions above.
Resources	• Preliminary opinion 5/2018 on Privacy by Design (31/05/2018) of the European Data Protection Supervisor, available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf • Data protection by design and default (23 May 2018), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ • Data Protection Measures by Design and By Default (March 2018), available at https://odpc.gg/wp-content/uploads/2018/05/DPByDesign.pdf • Guide, Software Development with Data Protection by Design and by Default (28 November 2017), available at https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/ • Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps (24 October 2012), available at https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/

	• Privacy Enhancing Technologies: Evolution and State of the Art. A Community Approach to PETs Maturity Assessment (9 March 2017), available at https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art/at_download/fullReport **Data Protection Impact Assessment (DPIA)** • 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, WP248 (4 April 2017), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 • Draft List of types of Data Processing Operations which require a Data Protection Impact Assessment (6 June 2018), available at https://www.dataprotection.ie/docimages/documents/DPIA%20for%20co nsultation.pdf • Data Protection Impact Assessments (15 May 2018), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/ • Data Protection Impact Assessments (2018), available at_http://gdprandyou.ie/data-protection-impact-assessments-dpia/ **Internet of Things** • Big Data and Smart Devices and Their Impact on Privacy (21 September 2015), available at_http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPO L_STU(2015)536455_EN.pdf
Synthesis	In groups of 5, the Students are required to create a PowerPoint presentation which outlines: (1) Their findings on the topic, (2) How they would update the existing SDLC and PMM workflows, and (3) A Target Operating Model (TOM). The proposal shall be shown to and discussed with the Head of IT of 'Get Well Soon' who may challenge the proposed approaches. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.
Reflections	The Students will be encouraged to reflect on the operational side of privacy and on how to foster awareness and accountability within the business. They will also be encouraged to think about how a similar scenario could be tackled more effectively in the future and record any individual reflections on the exercise.
Other notes	None.

3. Act	
Solution Prototypes	Each Group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this. The above-mentioned briefing shall include the following 1. An explanation of the Privacy by Design principles 2. How to make them live in the real world (i.e., strategies, tactics, privacy patterns) 3. A brief explanation of what is a Data Protection Impact Assessment (DPIA) 4. A Target Operating model (TOM) proposal 5. An updated PMM and SDLC process 6. Pros and cons of the suggested approach The recommendations provided should aim to improve attitudes to data privacy and security, as well as awareness of the implications of breaches of the privacy laws and regulations. The proposal shall be shown to and discussed with the Head of IT of 'Get Well Soon' who may challenge the proposed approaches. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.
Solution	The Students shall provide a solution or options for different solutions in the format suggested above.
Implementation plan	The Students shall provide a plan on how the solutions may be delivered, and how to foster a virtuous change management within the business.
Evaluate	The Students shall answer the following – 1. What are the strengths and weaknesses of the approach you have suggested? 2. How did you assessed the proposed trade-off between legal compliance and business needs? 3. What did you learn from this exercise? The Students will also be required to carry out a SWOT analysis on one of the suggested approaches.
Other notes	
4. Reflection and documentation	
Case notes	It can be developed in future by showing real SDLC and PMM processes and let the Students carry out a real Data Protection Impact Assessments (DPIAs).

Challenge Title: Data Management	
Use Case Author	Vittoria Russo, Maria Cristina Gaeta, Suor Orsola Benincasa University of Naples
Topic	Public Sector Legal
Overview	"Lalaland City Council" in Italy, is preparing to digitize all the archives to create a section in transparent administration, accessible through access by ID, by all citizens. The digitization service will be outsourced and managed by an external company, whose employees will directly process the personal data of the citizens. The data will be merged into a single platform and will be managed by employees of "Lalaland City Council".
1. Engage	
Big idea	Focus on data management and subsequent availability.
Essential Question	If you were a DPO in the "Lalaland City Council", what roles would you have assigned to the employees of the external company and then to the "Lalaland City Council" employees in the subsequent phases? What types of privacy policy would you give to citizens whose data are being processed? How would you have managed the next phase of access to the personal data?
Initial resources	Project work digitization: The main objective of the project is the digitization of documents in the municipal population register: individual cards, family cards, ID cards and civil status registers. The documents will be filed and managed in digital format, linked to the Demographic Services management application, making them accessible and searchable on video with considerable savings both in terms of direct costs (paper, spaces) and indirect costs (time, efficiency). The project involves the creation of a database containing the data of the resident population for the subsequent data implementation in the software that will manage the services of the municipal population register. The project will be divided into six phases: 1. Installation of software and driver scanners.

	2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2.Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria.

	Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized.

	At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria.

	Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized.

	At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria.

	Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively. 2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively.

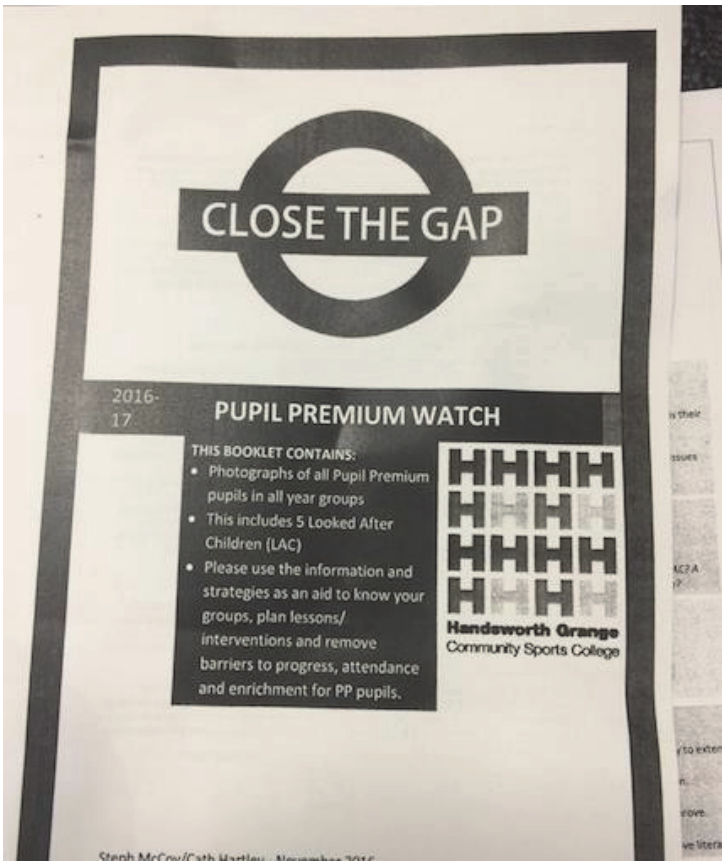
	2. Verification of the quantity, of the state of conservation and subdivision by type of the documents to be digitized. At the end of this phase, a report will be drawn upon the status of the documents and on the choice of those to be digitized in order to be delivered to the customer. 3. Digitization and implementation of the database with the insertion of all the data contained in the family cards, the individual ones and in the civil status registers. 4. Preparation of documents for scanning, verification, and correction of errors and association of image files. At the end of the acquisition and verification of the documents will be made, together with the Office Manager and the Customer, the choice of indexing criteria, which will be identified by the type of deeds. 5. Indexing according to the established criteria. Once the indexing phase is completed, while the service is being activated, the method for the extrapolation of the data from the municipal population register database for congruence checks is agreed. The extracted data are compared with those entered, proceeding to the manual correction of any anomalies. 6. The last phase will be used to test the functionality of the final product with the use of the application at the branches, after disclosure of the results within the Public Entity and the subsequent publicity on the website of the City Council. The project to be implemented requires the availability of technical tools such as: PCs and scanners that will be made available by the City Council, together with the material to be digitized and the human resources that will have to collaborate actively.
Guiding Questions	Jointly, the students have to act like they are the DPO of the "Lalaland City Council" and DPO of the company that will manage the digitization. Before going deep on the subject, they have to analyse the facts and wonder what the City Council exactly wants to achieve with the planned data operation. Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to develop a list of questions.
Reflections	According to the list of questions: Individual reflections on the process.

Other notes	Suggestions for dealing with the brainstorming exercise: 1. The teacher is the driver of the brainstorming exercise. 2. The teacher has to create an understanding atmosphere in which the students can express their ideas freely and confidently. The teacher and students have to respect others ideas, because all ideas, although it can be initially seen as nonsense, have value to address the suggested problem.
2. Investigate	
Activity Description	Encourage students to map out a process of the investigation they will follow for answering the questions above.
Resources	▪ Reading resource ▪ General Data Protection Regulation (sections from 44 to 49). ▪ Communication from the Commission to the European Parliament and the Council, The exchange and protection of personal data in a globalized world, COM (2017) 7 final/2 of 15.2.2017. ▪ Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Text with EEA relevance) (2003/490/EC) Encourage students to collect and use resources to help them to address the question. Establish a method for collecting information and organize the lectures. Make sure you meet your own ethical and data protection requirements.
Synthesis	In this second stage the students should form teams of 3 or 4 people. By groups, they should use the bibliographic resources provided to solve the different questions or problematic ideas that arose during the brainstorming, with the help of the mind maps created for this purpose. Then, a representative from each group will orally present the solutions they have given to the different issues. Once the different opinions have been expressed, a discussion session will be opened, in which the students will have to take into account the details of the case.

	Finally, each group of students will submit a paper (on a maximum of 6 pages) answering those questions. Encourage students to summarise their answer.
Reflections	Encourage dtudents to provide a reflection on the process: ▪ How have you been organized in small groups: each one had a task assigned or have you been improvising? ▪ Do you think it is important to express your conclusions in public? ▪ Do you think your communication skills are essential to the DPO work? ▪ Do you think this way of approaching the problem will help you to become a DPO? ▪ Would you undertake your advising work in a different way than you have done? (…)
Other notes	
3. Act	
Solution Prototypes	In order to carry out the DPO functions (sections 39.1 and 2 of the General Data Protection Regulation), students must individually prepare a report on the factual situation. The report should be structured as follows: [1] Factual background [2] Legal bases [3] Conclusions In addition, if it has been necessary to contact the Supervisory Authority, they must also point out those additional actions they have taken. At the end, one of these reports will be chosen and you will have to orally defend it before the commercial department of the company, indicating how they must legally act to be compliant with data protection rules and answering all their questions and doubts.
Solution	Students should have to provide a solution or options for different solutions in the format suggested above.

Implementation plan	Students also should have to provide a plan for how at least one of the solutions should be delivered.
Evaluate	Students should have to develop a journal entry to evaluate the different solutions, and how they might go differently about the exercise in future. • What are the key challenges for the company in order to implement the plan you have identified? • Have you taken into account all the challenges involved in international data transfers? • If the company decides to change the strategy and transfer the data to the branch office in Peru, would they know how to find a quick solution? • Students might also be asked how the exercise itself could be further developed as a pedagogical process. • Would you undertake this task in a different way than you have done? (…)
Other notes	
4. Reflection and documentation	
Case notes	

Challenge Title: Data Security and Mobilising the Whole School Workforce to close Educational Attainment Gaps	
Use Case Author	Alex Nunn, Tamsin Bowers-Brown, University of Derby
Topic	Public Sector
Overview	Schools in the UK are required to promote individual learning for all students. They are expected to provide challenge and 'stretch' for the most able students. They are also expected to address 'attainment gaps'between average attainment and groups which regularly attain below that. These groups differ over time but there is significant concern at the moment about white working class boys for example. Looked After Children (that is the UK term for children who are in the care of the local authority as opposed to their parents or other guardians) are also expected to receive additional attention, as are any pupils who may have'additional learning needs'. In order to target support at those pupils who need it the most, schools put a great deal of resource into generating attainment and progress data on their pupils. In order to use this to support pupils it needs to be shared with professionals who may work with the pupils, some of whom may work for the school, some of whom may be part time staff or students on placements, some may be visitors and work for the local authority and some may be private contractors or merely visitors to the school. The challenge is to support pupils in the most effective way, targeting support at those who need it most, while not contravening GDPR or DPA rules, and also not transgressing othe legal obligations such as 'safeguarding' or specific rules relating to Looked After Children or Equalities legislation.
1. Engage	
Big idea	Targeting support while keeping pupils and their data safe.
Essential Question	How can example primary school keep most effectively use pupil attainment and progress data to close attainment gaps while at the same time ensuring they and their data are safe and secure?
Initial resources	Educational Attainment Gaps: https://epi.org.uk/publications-and-research/closing-gap-trends-educational-attainment-disadvantage/



This is a brochure given to a placement student in a school. The booklet includes the names and photographs of pupils who are identified by the school as needing additional support, some of whom are identified as Looked After Children. There is also a notice board in the school hallway which has some of this same information presented on it.

Guiding Questions

You receive a call from a Headteacher at a local primary school where this brochure was produced and used. The placement student has complained that the booklet was being given to a range of people coming into the school including social workers, other placement students, a coach from a private football activity company and parents who sometimes come into school to help children with their reading. The placement student is concerned that this may not be compliant with the new GDPR rules. The Head

	Teacher wants to know what she should do. What questions should you ask of the Head Teacher to start to frame the task? Brainstorm a list of questions you should ask when you call the Head Teacher back.
Reflections	Complete your learning journal and answer the following questions: 1. What is interesting about this challenge? 2. How did you feel about the initial brainstorming exercise? 3. Were you happy with the list of questions you put together? Why/why not?
Other notes	
2. Investigate	
Activity Description	
Resources	Some resources to get you going: https://www.youtube.com/watch?v=y09IHXv6u6M&feature=youtu.be https://www.youtube.com/watch?v=RZUlsdyREvg&feature=youtu.be https://www.gov.uk/topic/schools-colleges-childrens-services/looked-after-children/latest https://www.gov.uk/government/publications/data-protection-and– privacy-privacy-notices https://ico.org.uk/for-organisations/education/ https://www.gov.uk/guidance/pupil-premium-information-for-schools– and-alternative-provision-settings https://www.gov.uk/children-with-special-educational-needs Please provide a list of additional resources that you have found and are useful in the task. Do you need to collect any other form of data? How will you collect this? Develop and implement a plan for collecting this information. Ensure that you meet your own Data Protection and ethical requirements.
Synthesis	Develop a short (maximum 5 pages) Booklet that school staff (e.g. teachers, Special Educational Needs Coordinator, Headteacher) can use to understand how they can balance the competing obligations for ensuring that pupil personal data is secure and that data is shared with those who need it to ensure that all those professionals who may work with them can contribute to closing educational attainment gaps.

Reflections	Please provide a reflective statement in your journal to summarise your answers to the questions below: 1. What are the key problems to be overcome in this challenge? 2. How did you organise the work involved in the investigation? 3. How did you collect additional data? What worked well about this? 4. What information gaps were still present at the end? 5. How successful was the investigation process? 6. How would you organise the work differently if you did it again?
Other notes	
3. Act	
Solution Prototypes	Design a project for a School Head Teacher can implement to ensure that staff and other professionals in their school meet their competing obligations to close educational attainment gaps and ensure data security. This might include: ▪ Data Protection Impact Assessment ▪ Training Data Sharing protocol
Solution	Please indicate your key recommendations to the Head Teacher here:
Implementation plan	Please develop a plan for the implementation of the project.
Evaluate	Please develop a journal entry which answers the following questions: 1. What are the key challenges for schools in implementing the plan you identified? 2. What were the strengths and weaknesses of your overall approach to the challenge? 3. Were there any changes that could be made to the booklet and the project implementation plan to make them more effective, based on your reflection on the whole challenge? 4. If you were to run this challenge with a group of learners, how would you change it? What else did you learn from this process?
Other notes	
4. Reflection and documentation	
Case notes	

Challenge Title: Responding to a Data Breach in a Bank	
Use Case Author	Andrew Morris, Martin Maguire, Nathan Stuttard, Loughborough University
Topic	
Overview	You are a member of the IT investigations department at a reputable bank. It has come to your attention that the data from a number of customers has been taken and their bank accounts have been hijacked. This came to light when several customers reported withdrawals from their accounts that they knew nothing about. As a result of this, the customers are extremely unhappy. It is possible that this has occurred due to a data analyst being careless, but you cannot be sure of this. Your supervisor has tasked you with investigating the cause of this data breach. Whether accidental or deliberate, it must be established how the breach occurred from a behavioural perspective. It is your task to determine the underlying reasons as to why the breach occurred, rather than simply what happened at the time.
1. Engage	
Big idea	Customers' personal data has been leaked and their bank accounts have been compromised.
Essential Question	How should the data analyst teams act to deal with the breach and to avoid such data breaches in the future? The big capstone question summarising the challenge.
Initial resources	The following links should provide some background to the problem. https://www.gutobebb.org.uk/news/computers-left-overnight-risk-cyber- attack https://www.tripwire.com/state-of-security/security-data-protection/5-innocent-mistakes-that-cause-an-it-security-breach/ https://www.shredit.com/en-us/blog/securing-your-information/january-2015/five-ways-employees-are-increasing-the-risk-of-a-s Any initial resources that students might use to contextualise the challenge – a video or reading exercise for example. This should not run into the investigation stage.

Guiding Questions	(1) How would you go about investigating the breach? (2) What actions by staff or others do you think caused the breach? (3) From the perspective of the data analyst, what do you think caused the breach? (4) How could you stop such a breach from happening in the future? (5) What actions would you need to take to report the incident? Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to develop a list of questions which break the challenge down into its constituent elements and manageable sections and to put these in an order. Use this space to show how you will do this and leave space for the students to complete the questions. This box should be completed as a team by the students
Reflections	Once the students have done this, encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge? How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process.
Other notes	
2. Investigate	
Activity Description	Encourage students to map out a process of investigation for answering the questions above.
Resources	List any reading, web or video resources here that you think would be good to 'get the students going'. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ https://www.kaspersky.com/blog/the-human-factor-in-it-security/ Other resources will include emailed complaints from customers, written statements from members of staff and logs of when staff left the building, based on door lock swipes. A report from the Bank's IT department will be also be provided.

	Searching through the following journals and databases may also help: Behaviour and Information Technology, Information and Management, Science Direct, Scopus, Taylor and Francis, Journal of Business Research and Computers and Security. Using multiple keyword combinations will assist with this. Encourage students to collect and use resources to help them to address the question.
Synthesis	The final product of this exercise should be a PowerPoint presentation to synthesise the students findings towards the problem. This should include a title and recommendations page. Establish a task – e.g. A presentation, report, essay, video, briefing etc that students should produce to synthesise their answer to the questions. Encourage students to summarise their answer.
Reflections	Students to provide a reflection on the process.
Other notes	
3. Act	
Solution Prototypes	Each group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this. This briefing will include information on the following: (1) The nature and cause of the breach (2) The implications and how they will be handled (3) The nature of the investigation, e.g. the measures used to reach the conclusion (4) Recommendations to the head of the Bank's Data Analysis and security division (5) Response will be provided to customers The recommendations provided should be based on a behavioural rationale and should aim to improve attitudes to data security and awareness of the implications of data breaches.
Solution	Students to provide a solution or options for different solutions in the format suggested above.

Implementation plan	Please provide a plan for the implementation of the project
Evaluate	Please address the following questions: 1. What are the key challenges for your organisation in implementing the plan you identified? 2. What were the strengths and weaknesses of your overall approach to the challenge? 3. Were there any changes that could be made to the company policy? What did you learn from this whole process?
Other notes	
4. Reflection and documentation	
Case notes	Your notes and reflections on how this challenge could be developed in the future.
	Gather class feedback from students about their experience in attending the class and conducting the exercise. If you were to run this challenge again with a group of learners, how would you change it?

Challenge Title: Protecting data from theft	
Use Case Author	Andrew Morris, Martin Maguire, Nathan Stuttard, Loughborough University
Topic	Public Sector Manufacturing
Overview	You are the head of the data breach Investigation department at the major manufacturing company, BigMetal. It has come to your attention that several reports have been stolen. These confidential reports contained the company's key innovation ideas, which are very important for future products. It is possible that this breach may have occurred due to human error, possibly through the paper reports unwittingly being left on a train, though you cannot be sure of this. Your supervisor has tasked you with investigating the cause of this data breach. If it was accidental, it must be established how the breach occurred from a behavioural perspective. It is your task to determine the underlying reasons as to why the breach occurred, rather than simply what happened at the time to cause it.
1. Engage	
Big idea	Clients' personal data has been stolen by hackers
Essential Question	How should the employees of BigMetal act to deal with the data breach and avoid such breaches in the future?
Initial resources	A few of these web links may be helpful: https://www.gutobebb.org.uk/news/computers-left-overnight-risk-cyber- attack https://www.tripwire.com/state-of-security/security-data-protection/5- innocent-mistakes-that-cause-an-it-security-breach/ https://ico.org.uk/for-organisations/guide-to-pecr/communications- networks-and-services/security-breaches/ https://simplicable.com/new/data-breach https://www.thedatacommander.com/single-post/2017/04/11/Manufacturing-is-2-Target-of-Cyber-Attacks https://www.youtube.com/watch?v=7i9KoamDmss
Guiding Questions	1. How would you go about investigating the breach? 2. What actions do you think caused the breach?

	3. From the perspective of the employee at BigMetal, what do you think caused the breach? 4. How could you stop such a breach from happening in the future? 5. What actions would you need to take to report the incident? Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to develop a list of questions which break the challenge down into its constituent elements and manageable sections and to put these in an order. Use this space to show how you will do this and leave space for the students to complete the questions. This box should be completed as a team by the students
Reflections	Once the students have done this, encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge? How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process.
Other notes	Any other notes that teachers and students should be aware of when using this challenge.
2. Investigate	
Activity Description	Encourage students to map out a process of investigation for answering the questions above.
Resources	List any reading, web or video resources here that you think would be good to 'get the students going'. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ https://www.calyptix.com/hipaa/top-5-causes-of-data-breaches-in- healthcare/ https://www.british-assessment.co.uk/guides/3-causes-security-breaches/ Other resources will include written statements from members of staff and descriptions from employees of how they recorded their passwords.

	Searching through the following journals and databases may also help: Behaviour and Information Technology, Information and Management, Science Direct, Scopus, Taylor and Francis, Journal of Business Research and Computers and Security. Using multiple keyword combinations will assist with this. Encourage students to collect and use resources to help them to address the question.
Synthesis	The final product of this exercise should be a PowerPoint presentation to synthesise the students' findings towards the problem. This should include a title and recommendations page. Establish a task – e.g. A presentation, report, essay, video, briefing etc that students should produce to synthesise their answer to the questions. Encourage students to summarise their answer.
Reflections	Students to provide a reflection on the process.
Other notes	Any other notes that teachers and students should be aware of when using this challenge.
3. Act	
Solution Prototypes	Each group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this. This briefing will include information on the following: (16) The nature and cause of the breach (17) The implications and how they will be handled (18) The nature of the investigation, e.g. the measures used to reach the conclusion (19) Recommendations to the management of BigMetal The recommendations provided should be based on a behavioural rationale and should aim to improve attitudes to data security and awareness of the implications of data breaches. (Provide the students with a format for presenting their solutions to the problem. This might be a report template, a real world simulated scenario – e.g. a briefing to a client or senior managers in an organisation).

Solution	Students to provide a solution or options for different solutions in the format suggested above.
Implementation plan	Please provide a plan for the implementation of the project Students also to provide a plan for how at least one of the solutions should be delivered.
Evaluate	1. Please address the following questions: 2. What are the key challenges for your Organisation in implementing the plan you identified? 3. What were the strengths and weaknesses of your overall approach to the challenge? 4. Were there any changes that could be made to the company Policy? 5. What did you learn from this whole process? Students to develop a journal entry to evaluate the different solutions, and how they might go about the exercise differently in future. Students might also be asked how the exercise itself could be futher developed as a pedagogical process.
Other notes	
4. Reflection and documentation	
Case notes	
	Gather class feedback from students about their experience in attending the class and conducting the exercise. If you were to run this challenge again with a group of learners, how would you change it?

Challenge Title: Ensuring Data Protection in the IoT domain	
Use Case Author	Aura Tardia, RE:Lab
Topic	Manufacturing
Overview	Provide a 100-300 word introduction to the challenge. Ensure that this only introduces the challenge and does not spell out solutions. You are the DPO of IoTech SA, a medium-sized company based in Brussels. The company develops IoT solutions to provide customers with efficient and useful connected objects, while also designing smartphone apps to allow the users to control and monitor the objects. The product developers are working on a pair of smart shoes which will be able to monitor the location of the wearer, the heartbeat, and other types of data and meta- data, in order to assist the user in getting to their destination safely and efficiently, suggest routes, monitor performance, etc. The shoes will gather the data and communicate with the wearer through the smartphone app. Even when the app is not in use, the shoes keep collecting the data and sending it to the central server.
1. Engage	
Big idea	One word or sentence about the challenge. Privacy and IoT
Essential Question	The big capstone question summarising the challenge'. How can IoT solutions be designed to ensure privacy protection?
Initial resources	Any initial resources that students might use to contextualise the challenge – a video or small reading exercise for example. This should not run into the investigation stage. These initial resources can help you frame the challenge at hand: http://www.dataprotection.ro/servlet/ViewDocument?id=1088 https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/ https://www.forbes.com/sites/nikkibaird/2017/08/31/if-consumer-privacy-isnt- already-dead-iot-could-kill-it/#2e4704ba2cf8 http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?IR=T
Guiding Questions	Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to de-

	velop a list of questions which break the challenge down into its constituent elements and manageable sections. And to put these in an order. The product developers are starting to work on the design of the smart shoes, and the project manager comes to you, as the company's DPO, to ask your advice and support on the topic. He knows that the new Privacy Regulation entails some changes, but he is not sure about what to do exactly in order to be compliant. Use this space to show how you will do this. And Leave space for the students to complete the questions. This box should be completed as a team by the students What questions should you ask the project manager to start to frame the task? Brainstorm a list of questions you should ask in order to get a clearer picture of the activity and of the role you could play. Draft a complete list of questions and put them in an order, prioritizing the ones you believe are more important.
Reflections	Once the students have done this. Encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge? How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process. Reflect on the Guiding Questions process and results: 1. How did you feel about the initial brainstorming exercise? 2. Were you happy with the list of questions you put together? Why/why not?
Other notes	
2. Investigate	
Activity Description	Encourage students to map out a process of investigation for answering the questions above. Now that you have identified the information you need from the project manager, you should collect the resources that can help you develop a good solution. The Investigation phase should lead you to the answers to your Guiding Questions.
Resources	List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_

	resolutionon_privacybydesign_en.pdf Practical approaches in the IoT domain: https://reader.elsevier.com/reader/sd/D5781B4CBC6BE33A9F678A1F8AA9BB12797C D3071EF8BFF4EAF4925A2EE9997C9C9A9375E664C3BBA7DCFCB48DB1BAD8 Encourage students to collect and use resources to help them to address the question. Try and gather more resources that can help you address the challenge more effectively.
Synthesis	Establish a task – eg. A presentation, report, essay, video, briefing etc that students should produce to synthesise their answer to the questions. Develop a presentation illustrating your Recommendations and Guidlines for the Product Development team to follow for the development of the smart shoes. This should allow them to understand how to concretely implement the principles and requirements of the GDPR. Try to focus on what data protection/privacy functions, sections, or specific elements the final object (and relate App) should (or should not) contain. Include them in your presentation. --- Encourage students to summarise their answer.
Reflections	Students to provide a reflection on the process. Reflect on the Investigation phase: 1. What are the key problems to be overcome in this challenge? 2. How did you organize the work for the presentation? 3. How did you collect additional information and resources? How successful was the investigation process? How would you organize the work differently if you did it again?
Other notes	
3. Act	
Solution Prototypes	Provide the students with a format for presenting their solutions to the problem. This might be a report template, a real world simulated scenario – e.g. a briefing to a client or senior managers in an organisation. Develop a project proposal, including control points, tentative timing and expected results, that the product developers should follow throughout the design of the new smart shoes.

Solution	Students to provide a solution or options for different solutions in the format suggested above.
Implementation plan	Students also to provide a plan for how at least one of the solutions should be delivered. Develop a plan for the implementation of the project. How will you monitor the progresses? What indicators will you evaluate? How will you cooperate with the product developers?
Evaluate	Students to develop a journal entry to evaluate the different solutions, and how they might go about the exercise differently in future. Students might also be asked how the exercise itself could be further developed as a pedagogical process. Develop a journal entry evaluating the solution you identified: 1. What are the key challenges that your colleagues may encounter in implementing the project? 2. What were the strengths and weaknesses of your overall approach? 3. What changes would you make to your solution? What did you learn from this process?
Other notes	
4. Reflection and documentation	
Case notes	

Challenge Title: Embedding Privacy in New Technologies	
Use Case Author	Roberto Montanari, Elisa Landini, Aura Tardia, RE:Lab
Topic	Data Protection
Overview	Provide a 100-300 word introduction to the challenge. Ensure that this only introduces the challenge and does not spell out solutions. AppOsta S.r.l., an Italian innovative small enterprise, is contracted by a big client the development of a mobile app. The app is intended to allow drivers to find, book and buy parking spots in urban areas using their mobile phone. AppOsta S.r.l. will implement state-of-the-art security measures for data protection within the app, which will gather personal data, location data and transaction data, among others.
1. Engage	
Big idea	One word or sentence about the challenge. Privacy and new technologies.
Essential Question	The big capstone question summarising the challenge'. How can technologies be designed to ensure privacy protection?
Initial resources	Any initial resources that students might use to contextualise the challenge – a video or small reading exercise for example. This should not run into the investigation stage. Many mobile apps still display information to the user in a way that is clearly non-compliant with the GDPR. Pre-ticked boxes are the most evident mistake. 

	In addition, many applications, even widespread ones, make it hard for the users to find their privacy settings, requiring them to navigate, tap and scroll through several pages before finding what they are looking for.  This means that the principles and processes of Data Protection by Design and by Default are still not fully known and understood by app developers and designers within enterprises.
Guiding Questions	Undertake a 'situation room' or 'briefing room' exercise with the students. They are your team. Encourage them to brainstorm to develop a list of questions which break the challenge down into its constituent elements and manageable sections. And to put these in an order. You are AppOsta S.r.l.'s newly appointed DPO. You are still collecting information to get acquainted with the company's activities and related data protection issues. The App Development Team is starting to work on the design of the Parking App, and the Team Leader comes to you, knowing that the app will deal with personal data. He's worried that he and his team do not know the new rules well enough to make the final app truly "GDPR compliant".

	The design process for the app has barely begun, so you have the opportunity to guide it in the right direction. --- Use this space to show how you will do this. And Leave space for the students to complete the questions. This box should be completed as a team by the students What questions should you ask the Team Leader to start to frame the task? Brainstorm a list of questions you should ask in order to get a clearer picture of the activity and of the role you could play. Draft a complete list of questions and put them in an order, prioritizing the ones you believe are more important.
Reflections	1. Once the students have done this. Encourage them to reflect on how well this exercise worked. How well do the questions reflect the challenge? 2. How could a similar situation be tackled more effectively in the future? Use this space to record individual reflections on the process. 3. Reflect on the Guiding Questions process and results: 4. How did you feel about the initial brainstorming exercise? Were you happy with the list of questions you put together? Why/why not?
Other notes	
2. Investigate	
Activity Description	Now that you have identified the information you need from the Team Leader, you should gather this information and collect the resources that can help you develop a good solution. The Investigation phase should lead you to the answers to your Guiding Questions.
Resources	List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr

	Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation:

	https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design:

	https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question.

	Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr

	Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation:

	https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design:

	https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question.

	Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr

	Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation:

	https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design:

	https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question.

	Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr --- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr

	Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr ---- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively. List any reading, web or video resources here that you think would be good to 'get the students going'. The principles of Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf General information on the topic: https://iapp.org/news/a/privacy-by-default-in-online-services/ Hints and tips on PbD implementation: https://www.information-management.com/opinion/how-to-implement- privacy-by-design-requirements-for-gdpr ---- Encourage students to collect and use resources to help them to address the question. Try and gather more resources that might help you address the challenge more effectively.
Synthesis	Establish a task – eg. A presentation, report, essay, video, briefing etc that students should produce to synthesise their answer to the questions. Develop a short document (5 pages max.) containing Guidelines for the Team to follow for the development of the Parking App. This should allow the Team to understand how to concretely implement the principles and requirements of the GDPR.

	Try to focus on what data protection/privacy functions, sections, or specific elements the final app should contain. Include them in the Guidelines. --- Encourage students to summarise their answer.
Reflections	1. Students to provide a reflection on the process. Reflect on the Investigation phase: 2. What are the key problems to be overcome in this challenge? 3. How did you organize the work for the development of the Guidelines? 4. How did you collect additional information and resources? 5. How successful was the investigation process? How would you organize the work differently if you did it again?
Other notes	
3. Act	
Solution Prototypes	Provide the students with a format for presenting their solutions to the problem. This might be a report template, a real world simulated scenario – e.g. a briefing to a client or senior managers in an organisation. Design a complete Workflow that the App Development team should follow throughout the design cycle. While each specific app will obviously require specific adaptations, this workflow should contain steps and processes that apply to app development in general and can be used as a basis for future cases within the company.
Solution	Students to provide a solution or options for different solutions in the format suggested above. Summarize your key recommendations and suggestions to the Team Leader for the development of the Parking App.
Implementation plan	Students also to provide a plan for how at least one of the solutions should be delivered. Please, develop a plan for the implementation of the Workflow solution. How will you monitor the progresses? What indicators will you evaluate? How will you cooperate with the App Development team?
Evaluate	Students to develop a journal entry to evaluate the different solutions, and how they might go about the exercise differently in future.

	Students might also be asked how the exercise itself could be further developed as a pedagogical process. Develop a journal entry evaluating the solution you identified: 1. What are the key challenges that the Team Leader and his colleagues may encounter in executing the Workflow? 2. What were the strengths and weaknesses of your overall approach? 3. What changes would you make to your specific Guidelines and to your general Workflow? What did you learn from this process?
Other notes	
4. Reflection and documentation	
Case notes	

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

LUCILLA GATT – Full Professor of Civil Law at Suor orsola Benincasa University of Naples, Director of EJPLT

ADRIÁN PALMA ORTIGOSA – Assistant Researcher at Seville University

ALEX NUNN – Professor of Global Political Economy at Derby University, member of the Scientific Committee member of EJPLT

ANDREW MORRIS – BSc in Psychology, MSc in Ergonomics, Ph.D. in Mechanical Engineering at Loughborough University, member of the Scientific Committee of EJPLT

AURA TARDIA – Project Manager at RE:Lab, member of the Editorial Team

DAVIDE BORELLI – Ph.D. in Law at Suor orsola Benincasa University of Naples, Tech/ Digital & Data Lawyer (Manager) at PricewaterhouseCoopers Legal United Kingdom, and Fellow at the International Association of Privacy Professionals (IAPP)

DEBORAH CAPUTO – Lawyer at MRPerugini law firm

ELISA LANDINI – Project Manager at RE:Lab

EMILIANO TROISI – Ph.D. candidate at Suor orsola Benincasa University of Naples

MARÍA BOCIO JARAMILLO – Assistant Researcher at Seville Universit

MARIA CRISTINA GAETA – Research Fellow in New Technology Law at Suor Orsola Benincasa University of Naples, Ph.D. in Law at Federico II University of Naples, Coordinator of the Editorial Team of EJPLT

MARIA ROBERTA PERUGINI – Lawyer and Privacy Professional, founder MRPerugini law firm

MARINÍ GAIA CHIACCHIO – Avvocato at the Court of Naples

MARTIN MAGUIRE – BSc in Computer Studies and MSc in Ergonomics at Loughborough University, Ph. D. in Human-computer interaction at Leicester Polytechnic, member of the Referees Committee of EJPLT

NATHAN STUTTARD – BSc and MSc in Psychology at University of Nottingham

ROBERTO MONTANARI – Co-founder and Head of R&D at RE:Lab, Professor of Interaction Design at Suor Orsola Benincasa University of Naples, member of the Scientific Committee of EJPLT

SUE JENNINGS – Head of Derby Law School at Derby University

TAMSIN BOWERS-BROWN – Associate Professor of Learning and Teaching at Derby University

VALERIA FALCE – Jean Monnet Professor of EU Innovation Policy and Full Professor of Regulation, Competition and Intellectual Property at the Europen University of Rome

VITTORIA RUSSO – Teaching Assistant in IT techniques and methodologies for lawyers at Suor Orsola Benincasa University of Naples

VERONICA CARRIERO – Ph.D. in Law at Parthenope University of Naples