Whistleblowing

Lachapelle, Amelie

Published in:
Deep diving into data protection

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Whistleblowing: Threat or Safeguard for Data Protection in the Digital Era?

Amélie Lachapelle[1]

Introduction

The current tragic events around the world in the context of the spread of COVID-19 are a poignant reminder of the need for serious consideration of latent alerts and dark precursors.

In the 2000s, French doctors had already tried, but unheard, to draw the attention of the French authorities to the need for more research on coronaviruses. Closer to us, the Chinese doctor Li Wenliang, who in December 2019 first raised the alarm about the seriousness of COVID-19 on social media, first attracted the wrath of the Chinese government, which saw it as "spreading rumours". He died in February 2020 of COVID-19.

Whistleblowing has become an essential factor in the running of digital democracy.

In the context of the digital society, the whistleblower Edward Snowden has shown that whistleblowing can significantly contribute to the respect of fundamental freedoms.

It must be noted that the GDPR, like the Police & Justice Directive, does not say a word about whistleblowing, as significant as the emergence of the figure of "whistleblower", as substantial as the practice of whistleblowing in a law enforcement system. On the other hand, the Directive on the protection of persons who report breaches of Union law (also referred to as the « Directive on whistleblowers »[2]) gives a central place to data protection in the European whistleblower protection regime. There is hope that data protection rules might contain unjustified alerts while supporting justified alerts[3].

---

[1] University of Namur, Faculty of Law, CRIDS/NaDI.

[2] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, *O.J.E.U.*, L 305/17, 26 November 2019.

[3] See namely CPVP, Recommendation n° 01/2006, p. 2, available at www.dataprotectionauthority.be/

After highlighting the specificities of whistleblowing in the digital age (I), the present chapter will explain the main limitations of the GDPR to the implementation of a whistleblowing mechanism (II) while showing how the GDPR encourages at the same time the implementation of a whistleblowing mechanism as an enforcement tool (III).

The neologism "whistleblowing" has given rise to many definitions. One definition, however, has received the approval of a majority of the doctrine[4]. It is the definition proposed by Marcia M. Miceli & Janet P. Near in 1985. "Whistleblowing" is defined as "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action"[5].

I. Whistleblowing in the Digital Era

For centuries, the press has offered publicity to reporting of malfunctions, as well as anonymity to those who are at the source of sensitive information. But this role as an "echo chamber" has taken a particular turn with the extraordinary growth of digital technology in recent decades. It can thus be said that the advent of whistleblowers in the 21st century is also associated with the development of information and communication technologies (hereinafter, "ICT")[6].

As Pierre Rosanvallon points out, the digital space is indeed particularly adapted – perhaps more – "to the functions of vigilance, denunciation and rating. Better still, the Internet is the realized expression of the

[4] In that sense, see namely T.M. Dworkin, "Foreword" in *International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown e.a., éd.), Cheltenham, Elgar, 2014; B. Fasterling, « Whistleblower protection: A comparative law perspective » *in International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown e.a., éd.), Cheltenham, Elgar, 2014, p. 334.

[5] J.P. Near & M.P. Miceli, "Organizational dissidence: The case of whistle-blowing", *Journal of Business Ethics*, Vol. 4, Iss. 1, 1985, p. 4.

[6] In that sense, see namely Conseil d'État français, *Le droit d'alerte : signaler, traiter, protéger*, Annexe 6 – Contribution du professeur Henri Oberdoff sur la notion d'alerte éthique, étude adoptée le 25 février 2016 par l'assemblée générale plénière du Conseil d'État, La Documentation française, 2016, p. 114 ; M. Bardin, « Les « lanceurs d'alerte » à l'ère du numérique :un progrès pour la démocratie ? » *in Protection des données personnelles et Sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?* (O. de David Beauregard-Berthier & A. Taleb-Karlsson, coord.), Bruxelles, Bruylant, p. 255; R. Bosua, S. Milton, S. Dreyfus & R. Lederman, '11. Going public: Researching external whistleblowing in a new media age' *in International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown e.a., éd.), Cheltenham, Elgar, 2014, pp. 253-254.

powers .... The Internet has become a generalized space for monitoring and evaluating the world. Far from being a mere instrument, it is the very function of surveillance"[7].

ICTs operate at two levels: at the level of the operation itself first (A) and at the level of the legitimacy of the operation second (B).

A. A New Way of Blowing the Whistle

It is clear that ICTs greatly facilitate the whistleblower's information gathering work. Digital information is now the primary form of information for an organization, and non-digital information can easily be digitized[8]. Moreover, the employees of a company or the agents of an administration are now all connected to an internal network and they generally have access to the Internet. Under these conditions, the transmission of information is extremely easy, both internally and externally. Whereas in the past denunciation was mainly based on rumour, it can now be backed up by hundreds, thousands or millions of supporting data.

The transmission of information is also more secure. In particular, anonymity makes it possible to get rid of the pejorative image of whistleblowing, while at the same time protecting oneself from reprisals related to the disclosure of confidential information outside the insider community. The WikiLeaks platform, created in 2006, offers such anonymity by relying on the TOR network[9], TAIL software[10] and financing via encrypted currencies such as Bitcoin[11]. Other digital tools are now based on the same technology. These include www.sourcesure.eu, the site for anonymous sending of confidential documents to the media[12], the "EuLeaks" platform, launched by Greens/EFA Group in the European

[7] In French, read: « aux fonctions de vigilance, de dénonciation et de notation. Mieux, Internet est l'expression réalisée des pouvoirs …. Internet est devenu un espace généralisé de veille et d'évaluation du monde. Loin de constituer un simple instrument, il est la fonction même de surveillance » (P. Rosanvallon, *La contre-démocratie, la police à l'âge de la défiance*, Paris, Seuil 2006, p. 75). About the digital democracy and the concept of « cyber-résistance », see H. Oberdoff, *La démocratie à l'ère du numérique*, Grenoble, P.U.G., 2010, p. 96.

[8] R. Bosua, S. Milton, S. Dreyfus & R. Lederman, *op. cit.*, p. 253.

[9] The name derives from the acronym of the original software project, entitled "*The Onion Router*".

[10] "*The Amnesic Incognito Live System*".

[11] The funding of the WikiLeaks organisation relies entirely on the public. Donations can be made via the secure and anonymous *Bitcoin* virtual currency, for example (see "Donate to WikiLeaks", https://shop.wikileaks.org/donate, accessed April 13, 2018).

[12] Accessed March 20, 2020.

Parliament[13] and the GlobaLeaks platform, which provides anonymous and secure alerting and is used by more than 60 organizations around the world, including "independent media, activists, public bodies, companies and more"[14].

New technologies facilitate the whistleblower's analytical work, making it easier to find and cross-check relevant information. Search engines provide the potential whistleblower with the opportunity to quickly gather information before resorting to internal or external reporting[15]. In the same way, technological tools also make it easier for the recipients of the alert to use and disseminate the received information.

In this respect, the monumental work carried out by the International Consortium of Investigative Journalists (ICIJ) on the "*Panama Papers*", thousands of pieces of data from the *Mossack Fonseca* law firm, illustrates the importance of technological tools in journalistic work, both to guarantee the anonymity of whistleblowers and to allow the processing of thousands of pieces of data in the four corners of the planet. The book written by the two German journalists contacted by the "*Panama Papers*" whistleblower explains in detail – but not too much for obvious issues of confidentiality, security and competition – their methodology and the techniques they employed[16].

B. A New Way of Thinking about Whistleblowing

On the other side, ICTs are also likely to contribute to the legitimacy of whistleblowing.

First of all, ICTs allow the whistleblower to easily substantiate his or her allegations, where the informer had to or could formerly be satisfied with rumours. The reliability of reporting was then largely marred by this, and vile feelings could disguise the informer to the point where it was reduced to pure snitching. By increasing the reliability of the information, denunciation has become more legitimate in the eyes of society which, without fully endorsing the act, no longer systematically sees it as an act of snitching.

---

[13] Available at www.greens-efa.eu/ (accessed June 10, 2017). However, the website no longer seems to be active since 2018.

[14] Homepage of *GlobaLeaks*, available at www.globaleaks.org/fr/ (accessed February 25, 2018). See for example *PubLeaks*, *WildLeaks* et *MafiaLeaks*.

[15] R. Bosua, S. Milton, S. Dreyfus & R. Lederman, *op. cit.*, p. 253.

[16] B. Obermayer & F. Obermaier, *Le secret le mieux gardé du monde. Le roman vrai des Panama Papers*, Paris, Seuil, 2016.

Secondly, cases such as "*Snowden*" and "*Cambridge Analytica*" have revealed to the world that ICTs allow public authorities and private companies to massively collect personal data. These massive collections are the basis for what Antoinette Rouvroy calls the "algorithmic governmentality"[17], i.e. a new form of governance based on the mathematical results obtained from data manipulation. In such a context, whistleblowing is, according to Alfred de Zayas, a UN expert, a bulwark to thwart the actions of a "Big Brother" in the making[18]. The two cases mentioned above – the first concerning the massive surveillance carried out by governmental organizations using personal data held by private operators; the second concerning the misappropriation of personal data by private operators in charge of communicating electoral campaigns – are a striking illustration of this.

Some authors also believe that it is the development of ICT and the risks associated to it that has really motivated the European legislator to tackle the problem of whistleblowers[19]. The "*Snowden*" and "*Cambridge Analytica*" cases have actually hit Europe on key policies, both by their nature and scope, as well as by the different approaches they give rise to in Europe and the United States: intelligence and personal data protection.

II. GDPR, a Limit to Whistleblowing

While the GDPR completely ignores the issue of whistleblowing, the Directive on whistleblowers gives an important place to the GDPR and the protection of personal data. The right to the protection of personal data, and especially the requirement of confidentiality, occupies a cardinal place in the European whistleblower protection regime (A)[20], and

[17] A. Rouvroy, « Face à la gouvernementalité algorithmique, repenser le sujet de droit comme puissance », 2012, available at http://docslide.fr/ (accessed June 10, 2017).

[18] A.-M. de Zayas, "Human Rights and *Whistleblower*" Human Rights Council side-event, Monday 23 March 2015, p. 6, available at www.ohchr.org/ (accessed November 1st, 2016). See also F. Chateauraynaud, « Lanceur d'alerte », *in Dictionnaire critique et interdisciplinaire de la participation* (I. Casillo with R. Barbier, L. Blondiaux, F. Chateauraynaud, e.a., eds), Paris, GIS Démocratie et Participation, 2013, available at www.dicopart.fr (accessed May 17, 2017).

[19] In that sense, see M. Bardin, *op. cit.*, p. 255.

[20] See namely Recitals 14, 82, 83, 84 & 85 and Articles 16 & 17 of the Directive on whistleblowers. See also Article 32(2)(c) of the Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, *O.J.E.U.*, L 173/1, 12 June 2014; Recitals 41 & 43 of the Directive (EU) 2015/849 of the European

for good reason: the operation of a whistleblowing system involves, in almost all cases, the processing of personal data relating to a natural person within the meaning of the European data protection regulations (B).

A. A Key Component of European Whistleblower Protection

The *Snowden* affair, named after the whistleblower behind the scandal, was sufficient proof that the United States and Europe greatly differ in their approach to privacy and data protection[21]. Because of the unspeakable abuses committed in particular during the Second World War, the European legal tradition is marked by the need to protect individuals with regard to the processing of personal information.

Whistleblowing, at first a corporate reporting mechanism, was initially introduced in the European continent at the occasion of the implementation of the American *Sarbanes-Oxley Act*[22]. Whistleblowing has its roots in the Anglo-Saxon legal tradition of "*Qui Tam*". While this principle is certainly inspired by the mechanism of popular accusation set up in Ancient Greek and Roman times, it should be pointed out that it was abandoned in Europe during the Middle Ages because of its many incongruities[23]. In addition, it should be recalled that the Nazi regime, whose totalitarian practices also motivated the elaboration of a specific protection of natural persons with regard to the processing of personal data, has precisely established the denunciation as a government technique, including in occupied territories such as France and Belgium[24].

Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *O.J.E.U.*, L 141/73, 5 June 2015; Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, "Fighting Corruption in the EU", 6 June 2011, COM(2011) 308 final, p. 13, point 4.1.3.

[21] European authorities frequently refer to it when explaining European data protection rules. See namely Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données. Édition 2018*, Luxembourg, Office des publications de l'Union européenne, 2019, pp. 50 et 286.

[22] See namely D. B. Lewis, "Whistleblowing and data protection principles: is the road to reconciliation really that rocky?", *E.J.L.T.*, Vol 2, No. 1, 2011, pp. 1-15.

[23] About the history of the « *Qui Tam* », see namey J. Randy Beck, "The False Claims Act and the English Eradication of Qui Tam Legislation", *North Carolina Law Review*, 2000, Vol. 78, Nbr 3, Art. 2, pp. 539-642. About the history of denunciation in Europe, see A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale : de la complaisance à la vigilance*, Bruxelles, Larcier, 2021, pp. 71-124.

[24] About the denunciation during the German occupation, see L. Joly, « La délation antisémite sous l'Occupation », *Vingtième Siècle. Revue d'histoire*, 2007, n° 4, pp. 137-149;

These factors explain the initial outcry against whistleblowing in Europe, as well as the political focus on compliance with privacy and data protection requirements.

The French data protection authority originally strongly condemned whistleblowing, considering that its implementation in Europe "could lead to an organised system of professional denunciation"[25]. But after emotion often comes reason. It must be acknowledged that European data protection rules, which are very recent in terms of the history of law, usefully complement or reinforce the principles established by the European Court of Human Rights on the right to freedom of expression with regard to "whistleblowing cases".

The legal framework of the whistleblower phenomenon with regard to the right to privacy and to data protection now represents a major challenge to avoid unjustified alerts and to encourage justified alerts[26]. Compliance with data protection is also likely to strengthen alert mechanisms because of the guarantees such protection entails in terms of confidentiality, transparency and security[27].

B. Whistleblowing Compliance with Data Protection

As stated earlier, the operation of a whistleblowing system usually creates a situation in which European data protection rules, and especially those from the GDPR, are applicable insofar as such a system involves the collection and processing, in whole or in part by automatic means, of personal data relating to identified or identifiable natural persons (employees, managers, trainees, etc.).

Data protection rules have to be respected not only by organisations, public or private, which set up such mechanisms, but also in principle by persons acting as whistleblowers.

L. Joly, *Dénoncer les Juifs sous l'Occupation*, Paris, CNRS, 2017 ; L. Joly (ed), *La Délation dans la France des années noires*, Paris, Perrin, 2012.

[25] In French, read "pourrait conduire à un système organisé de délation professionnelle" (CNIL, Délibération n° 2005-110 du 26 mai 2005 relative à une demande d'autorisation de McDonald's France pour la mise en oeuvre d'un dispositif d'intégrité professionnelle, p. 4). See also CNIL, Délibération n° 2005-111 du 26 mai 2005 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en oeuvre d'un dispositif de "ligne éthique", p. 3, available at www.cnil.fr/en/home.

[26] See namely CPVP, Recommendation n° 01/2006, p. 2, available at www.dataprotectionauthority.be/.

[27] In this sense, see namely CEPD, Lignes directrices du 18 juillet 2016, p. 4, point 3; WP29, Opinion No 1/2006, p. 20.

The Directive on whistleblowers does not exclude that a whistleblower may be prosecuted for breaching personal data protection rules[28]. However, the whistleblower should be able "to rely on having reported breaches or made a public disclosure in accordance with this Directive as a defence, provided that the information reported or publicly disclosed was necessary to reveal the breach"[29].

Internal whistleblowing systems set up by public and private organizations are not the only systems that are subject to European rules. Whistleblowing is not limited to internal reporting. It encompasses other reporting channels, such as external reporting and public disclosure[30]. In this case, reporting to the prosecuting authorities is likely to create a situation subject to the rules of the Police & Justice Directive[31], whereas public reporting should be subject to the derogatory rules governing activities for journalistic purposes.

In any event, the organization, whether a company, public authority or media organisation, which sets up a whistleblowing mechanism must comply with the basic principles of data protection as consolidated in the GDPR. These principles relate to three essential aspects of protection[32]: the lawfulness of data processing (1), the principles relating to data processing (2) and the rights of the data subject and their restriction (3)[33].

1. The Lawfulness of Processing of Personal Data

All data processing must be lawful. To be lawful, the processing must be based on a legitimate basis as laid down in Article 6(1) of the GPDR. When the processing relates to certain particularly sensitive data, the GPDR furthermore obliges the controller to have a further basis for lawfulness.

[28] Recital 97 of the Directive on whistleblowers.

[29] Recital 97 *in fine* of the Directive on whistleblowers.

[30] See namely R. Bosua, S. Milton, S. Dreyfus & R. Lederman, "11. Going public: Researching external whistleblowing in a new media age" *in International Handbook on Whistleblowing Research* (Lewis D., Brown A.J., e.a., eds.), Cheltenham, Elgar, 2014, pp. 250-272.

[31] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.E.U.*, L 119, 4 May 2016.

[32] We will address the implementation of the "accountability principle" in the framework of point III "GDPR, an incentive to blowing whistle".

[33] About the application of data protection to whistleblowing, see A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, *op. cit.*, pp. 1071-1177.

Three grounds are likely to justify all data processing carried out in the context of a reporting system.

First, data processing carried out in the context of a reporting system will usually be considered as lawful if it is "necessary for compliance with a legal obligation to which the controller is subject"[34].

As the law currently stands, the obligation to establish an internal alert system exists for the private sector in most Member States of the European Union with a view to better regulate the banking sector[35]; to better fight market abuse[36], money laundering and terrorist financing[37]; to better ensure the safety of offshore oil and gas operations[38] and civil aviation[39].

The recent Directive on whistleblowers extends the obligation to a multitude of other areas of EU law, including the protection of privacy and personal data, the security of network and information systems, the public health, the protection of the environment, the food and feed safety, animal health and welfare and the fight against tax fraud and tax evasion[40].

The public sector is currently concerned in one main area, namely the fight against corruption. This area is not regulated by any *hard law* instrument in EU law[41], but most Member States have national legislation on

[34] Article 6(1)(c) of the GPDR.

[35] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, *O.J.E.U.*, L 176/338, 27 June 2013 and Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), *O.J.E.U.*, L 335/1, 17 December 2009.

[36] Market abuse regulation, *supra*.

[37] Fourth Anti-Money Laundering Directive, *supra*.

[38] Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC, *O.J.E.U.*, L 178/66, 28 June 2013, Article 22, Recital 41 et Annex IV.

[39] Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007, *O.J.E.U.*, L 122/18, 24 April 2014.

[40] Article 2(1) of the Directive on whistleblowers.

[41] On this subject, the European bodies refer to the work of the UN, the Council of Europe and the OECD. It should be noted that their work is aimed at both public and private sector workers. See namely "EU Anti-Corruption Report", 3 February 2014, COM(2014) 38 final.

the subject[42]. The Directive on whistleblowers, applicable to both the private and public sectors therefore considerably broadens the obligations to this sector.

Second, data processing carried out in the context of a reporting system will usually be considered as lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party"[43].

Since the processing of personal data by public authorities must be based on a *legal basis*, a public authority could not justify the establishment of a whistleblowing arrangement as being necessary for the pursuit of its *legitimate interests*[44].

In contrast, companies could claim that the implementation of such a system pursues their legitimate interests in that it contributes to consolidate good corporate governance. Whistleblowing is definitely today a tool for corporate social responsibility[45]. However, such a basis is only valid insofar as the interests, freedoms or fundamental rights of the data subject with regard to the protection of personal data do not prevail[46]. In any case, appropriate safeguards must be provided in practice in order to maintain a fair balance between the legitimate interests pursued by the data controller and the fundamental rights of the data subject[47].

Third, data processing carried out in the context of a reporting system will be considered as lawful if it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"[48].

---

[42] For instance, see in Belgium the "Loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel", *M.B.*, 4 October 2013. France, for its part, has chosen to limit itself, initially, to workers in the private sector (Article 9 of the "Loi française n° 2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption", *J.O.R.F.*, 14 November 2007). Nevertheless, the "Sapin II Law" has since established a genuine general legal regime for the protection of whistleblowers.

[43] Article 6(1)(f) of the GPDR.

[44] Recital 47 and Article 6(1) *in fine* of the GDPR.

[45] See namely S. Charreire Petit & J. Surply, « Du whistleblowing à l'américaine à l'alerte éthique à la française: enjeux et perspectives pour le gouvernement d'entreprise », *M@n@gement*, 2008/2, Vol. 11, pp. 113 à 135; A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, *op. cit.*, pp. 152-156.

[46] Article 6(1)(f) *in fine* of the GPDR.

[47] WP29, Opinion No 1/2006, p. 10. In particular, it should be noted that Article 21(1) of the GDPR provides that the data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data relating to him or her on the basis of Article 6(f) of the GDPR.

[48] Article 6(1)(e) of the GPDR.

An example is the processing of personal data collected via a tax report. Such processing undoubtedly contributes to the completion of the tax authorities duties, in this case to the establishment and collection of taxes[49], with the understanding that Article 3(1) of the Belgian Law of 3 August 2012 on provisions relating to the processing of personal data carried out by the Federal Public Service Finance in the context of its tasks states that the "Federal Public Service Finance collects and processes personal data in order to carry out its legal tasks"[50], that is to say the establishment, control, collection and recovery of taxes[51].

2. The Principles relating to Processing of Personal Data

Article 5(1) of the GDPR lays down the principles relating to the processing of personal data. These principles can be summarised around five key principles: transparency, fairness, purpose, proportionality, integrity and confidentiality.

Responsibility for compliance with these principles lies with the organization that decides, or is required, to set up a reporting mechanism (data controller) and, where applicable, with its service provider (processor).

As a keystone of the regime for the protection of both personal data[52] and whistleblowers[53], the *principle of transparency* requires that a precise description of the whistleblowing procedure be made available to the organization's employees who may be involved in the system, i.e. the organization's employees, but not only since the whistleblowing system can be extended to other persons having contact with the organization (whistleblowers "*sensu lato*")[54]. Such transparency is part of the awareness

[49] That being so, it must be conceded that the Law of 3 August 2012 is not really eloquent when it refers to "legal missions". To get an idea of these missions, it is useful to consult the parliamentary work on the Bill relating to certain processing of personal data by the Federal Public Service Finance of 2007, which was aborted due to the long political crisis in Belgium after the federal parliamentary elections of 13 June 2010 (see Projet de loi relatif à certains traitements de données à caractère personnel par le Service Public Fédéral Finances, Exposé des motifs, *Doc.*, Ch., 2006-2007, n° 51-3064/001, pp. 10-16).

[50] Loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.*, 24 August 2012.

[51] Explications de la partie 1 du document préparatoire à la déclaration à l'impôt des non-résidents (personnes physiques), Exercice d'imposition 2017 (revenus de l'année 2016), p. 137, available at https://finances.belgium.be (accessed December 11, 2019).

[52] Article 5(1)(a) of the GDPR.

[53] See especially Recitals 75 & 89 of the Directive on whistleblowers.

[54] Article 8(2) of the Directive on whistleblowers.

raising effort that must necessarily accompany the implementation of a reporting system, for reasons of efficiency[55].

The *principle of fairness* further implies that "data processing may not be carried out without the knowledge of the data subjects, in a manner which would be wholly unexpected or unforeseeable for them. Data subjects must be able, in full knowledge of the facts, to establish a relationship of trust with those who process their personal data"[56].

By guaranteeing the relationship of trust that unites the people involved in the reporting process, the requirement of loyalty may be seen as a counterbalance to the risks that the implementation of reporting systems within an organisation poses to the quality of corporate relations.

As already stated under the previous Privacy Directive, personal data must, in accordance with the *principle of purpose*, be collected for "specified, explicit and legitimate purposes". It follows that the processing carried out in the context of a reporting scheme must "serve a specific purpose and be justified in the light of the organisation's tasks and activities"[57].

When the lawfulness of the reporting system is based on a legal obligation or the pursuit of a public interest task, the purpose of the processing operation carried out in the framework of the reporting system must be precisely defined by the lawmaker[58]. When the reporting system bases its lawfulness on the legitimate interest of the controller, it is for the controller to define the purpose of the processing operation.

It is also important that personal data processed in the context of a whistleblowing mechanism are, in accordance with the *principle of proportionality and minimisation*, "adequate, relevant and limited to what is

[55] Since the establishment of reporting mechanisms is foreign to our legal culture, the effort to raise awareness is particularly important and conditions the effectiveness of such reporting mechanisms, beyond the construction of a legal framework. About this need for awareness, see namely Recommendation CM/Rec(2014)7, Appendix to Recommendation CM/Rec(2014)7, Principles 27 et 28.

[56] In French, read: les "traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données, d'une manière qui serait tout à fait inattendue ou imprévisible pour elles. Les personnes concernées doivent, en pleine connaissance de cause, pouvoir établir une relation de confiance avec ceux qui traitent leurs données à caractère personnel" (C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité » in Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie (C. DE TERWANGNE & K. ROSIER, eds), 1ère éd., coll. du CRIDS, Bruxelles, Larcier, 2018, p. 88).

[57] In French, read: "répondre à un objectif précis et être justifié au regard des missions et des activités de *l'organisme*" (CNIL, Projet de référentiel du 11 avril 2019, p. 3, available at www.cnil.fr/en/home).

[58] Article 6(3) of the GDPR.

necessary in relation to the purposes for which they are processed"[59] and "accurate and, where necessary, kept up to date"[60]. The GDPR specifies that "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"[61].

In particular, the late Belgian Privacy Protection Authority stressed that the data should be limited to the designation of facts and should not, in principle, contain value judgments or subjective assessments. It should expressly mention that they concern unproven facts[62]. The French Data Protection Authority also specifies that the following data may be collected as part of a whistleblowing system: "(a) identity, functions and contact details of the issuer of the occupational alert; (b) identity, functions and contact details of the persons who are the subject of an alert; (c) identity, functions and contact details of the persons involved in collecting or processing the alert; (d) facts reported; (e) elements collected in the context of the verification of the facts reported; (f) reports on verification operations; (g) action taken in response to the alert"[63].

Finally, the controller and the processor are required to process personal data, in accordance with the *principles of integrity and confidentiality*, "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"[64] .

Among the recommended "appropriate" measures[65], the confidentiality of the identity of the whistleblower, the person accused, and the information reported is a major guarantee within the protection system

[59] Article 5(1)(c) of the GPDR.

[60] Article 5(1)(d) of the GPDR.

[61] Article 5(1)(d) *in fine* of the GPDR.

[62] CPVP, Recommandation n° 01/2006, pp. 6 et 7, available at www.dataprotectionauthority.be/. In this sense, see also CNIL, Projet de référentiel du 11 avril 2019, p. 5, available at www.cnil.fr/en/home.

[63] In French, read : "a) identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ; b) identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ; c) identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ; d) faits signalés ; e) éléments recueillis dans le cadre de la vérification des faits signalés ; f) comptes-rendus des opérations de vérification ; g) suites données à l'alerte" (CNIL, Projet de référentiel du 11 avril 2019, p. 5, available at www.cnil.fr/en/home). The "référentiel" has been adopted on 18 July 2019.

[64] Article 5(1)(f) of the GPDR.

[65] For a detailed list of security measures to be taken by the controller in the context of a reporting scheme, see CNIL, Projet de référentiel du 11 avril 2019, p. 11. See also the *Guide de la sécurité des données personnelles* (edition 2018) available at www.cnil.fr/en/home.

developed by both the European data protection authorities and the European lawmaker. In particular, it appears that the whistleblowing system cannot be effective, given the risks of reprisals against the whistleblower, if the whistleblower fears that their identity and the content of their reporting could be revealed to third parties.

3. The Data Subject's Rights

The concerned parties, i.e. the whistleblower, the person against whom the reporting is made and the possible third parties – such as "facilitators" within the meaning of the Directive on whistleblowers – enjoy, as a rule, the "rights of the concerned person" provided for in Chapter III of the GDPR.

Data subject rights include the right of information, the right of access, the right of opposition, the right to rectification and the right to erasure ("right to be forgotten")[66]. The effectiveness of these rights depends upstream on individual information to be given to the data subjects. The right of information therefore occupies a special place among the rights conferred on the data subject.

The right to data protection is recognized only for natural persons[67]. Thus, if the company or institution shaken by a report may suffer prejudice, particularly in the event of a breach of confidentiality, it will have to rely on other legal resources, such as the law of liability but also now the whistleblowing law[68].

Insofar as the right to protection of personal data is closely linked to the right to privacy, enshrined in Article 7 of the Charter of Fundamental Rights of the EU, the limitations that may legitimately be made to this right correspond to those tolerated under Article 8 of the ECHR. This fundamental principle, which guarantees consistency between the protection conferred by the Council of Europe and that conferred by the EU, is reflected in Article 23 of the GDPR.

---

[66] About the rights of the data subject, see namely T. Tombal, « Les droits de la personne concernée dans le RGPD » *in Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (C. de Terwangne & K. Rosier, eds), 1ère éd., coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 407-558.

[67] According to Article 1(1) of the GDPR, the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data".

[68] Indeed, the Directive on whistleblowers protects from retaliation legal entities belonging to or working for whistleblowers, or with which they are connected in a professional context (Articles 19 & 4 of the Directive).

In addition to the specific limitations to one or the other right provided for directly in the provisions of the GDPR enshrining those rights, Article 23(1) of the GDPR provides, in a cross-cutting manner, that the EU law or the law of the Member State to which the controller or processor is subject may limit the scope of the rights of the data subject "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard" an important objective of general public interest of the Union or of a Member State[69].

The protection of the rights and freedoms of other persons involved in the whistleblowing mechanism is one of these objectives. This assumption is included in the GDPR in Article 23(1)(i). The Directive on whistleblowers specifies, in this respect, in Recital 84, that the effective protection of the confidentiality of the identity of the whistleblowers must be considered necessary for the protection of the rights and freedoms of others. Confidentiality is indeed an essential *ex ante* measure to avoid reprisals[70].

III. GDPR, an Incentive to Blowing Whistle

European authorities have learned the lessons of the *Snowden* case: data protection rules limit as much as they justify the deployment of whistleblowing.

As mentioned above, the Directive on whistleblowers explicitly lists the protection of privacy and personal data, as well as the security of networks and information systems, amongst the matters whose reporting is protected[71]. It results in a right of reporting in this area for the workers. The French Council of State, in its annual study of 2014, already recommended the introduction of a right of reporting in terms of data protection rather than the strengthening of the powers of the "CIL" ("*Correspondant Informatique et Libertés*"), the French equivalent of the Data Protection Officer (hereinafter: "DPO")[72].

[69] It should be noted that the EDPS has developed guidelines to facilitate the assessment of the proportionality of measures restricting the rights of the data subject. See EDPS, *Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 December 2019, available at https://edps.europa.eu.

[70] Recital 82 of the Directive on whistleblowers.

[71] Article 2 and Recital 14 of the Directive on whistleblowers.

[72] Conseil d'État français, Rapport 2014: « Le numérique et les droits fondamentaux », Proposition n° 7, p. 282.

In the light of these considerations, the right of data subjects to express their concerns to the DPO, provided for in Article 38(4) of the GDPR (A), but also the right of the workers to blow the whisle in terms of data protection in compliance with the Directive on whistleblowers should be understood as a right of reporting. The implementation of this right implies the setting up of a whistleblowing mechanism (B).

A. The New Faces of Compliance

While it may be preferable to entrust the management of reporting to a person directly designated for this purpose, the Directive on whistleblowers provides that the functions of "*Whisteblower Officer*" may be exercized by both the *Compliance Officer* and the *Data Protection Officer* on the condition that the latter have the appropriate qualifications[73]. The DPO is, in any case, entitled to receive the concerns of data subjects with regard to their rights as recognized by the GDPR[74].

Besides the function of Compliance Officer, the functions of DPO and Whistleblower Officer are new figures of "compliance (management)"[75]. These three functions enjoy similar legal guarantees, particularly in terms of professional qualification, confidentiality, and independence. The DPO[76], the Whistleblower Officer[77] and the Compliance Officer[78] also carry out their duties under the responsibility of the effective management of the organization in which they work. The responsibility for compliance with the respective legislation – data protection, legislation

[73] Recital 56 of the Directive on whistleblowers. The proposal for a directive of 23 April 2018 already envisaged such a solution (Recital 45). At the same time, Article 38(6) of the GDPR allows the DPO to carry out other tasks and duties under the condition that these do not give rise to a conflict of interest. For some reservations, see A. LACHAPELLE, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, *op. cit.*, n° 902.

[74] Article 38 (4) of the GDPR.

[75] Originally from Anglo-Saxon countries, the compliance function emerged in the financial sector in the 1990s. It has since then expanded to other areas, such as competition and the environment. On the subject, see namely M.-A. FRISON-ROCHE (dir.), *Régulation, supervision, compliance*, Paris, Dalloz, 2017.

[76] See namely K. ROSIER, « Délégué à la protection des données: une nouvelle fonction, un métier en devenir » *in Vers un droit européen de la protection des données* (B. DOCQUIR, ed.), Bruxelles, Larcier, 2017, p. 136.

[77] This emerges from the logic that precedes the setting up of a reporting system, which is for the organization, to ensure compliance with the legislation to which it is subject.

[78] See for instance in Belgian law, Article 87*bis* (1)(2) of the "Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers" and Article 1, 8° of the "Règlement de l'Autorité des services et marchés financiers relatif à l'agrément des *compliance officers* du 20 juillet 2016" (approved by the Arrêté royal of 9 August 2016, *M.B.*, 8 September 2016).

designated in the whistleblower system and financial and banking legislation[79] – remains with the concerned company.

These considerations make it possible to take the measure of the ambivalence which may affect the function of Data Protection Officer: the latter may be public official, whistleblower officer and whistleblower:

- sometimes a *public official*, in that the DPO "facilitates" compliance with the provisions of the Regulation within the organisation of the controller[80] and acts as a contact point for the supervisory authority[81] ;
- sometimes a *whistleblower officer* since the DPO may receive complaints on infractions from the workers and the data subjects regarding the processing of personal data and the exercise of their rights under the GDPR[82] ;
- sometimes a *whistleblower*[83] in that the DPO "shall directly report to the highest management level of the controller or the processor"[84] and shall "cooperate with the supervisory authority"[85].

This ambivalence, that may threaten the DPO in the performance of his tasks, explains why the European lawmaker saw it fit to provide that the DPO shall not be "dismissed or penalised by the controller or the processor for performing his tasks"[86].

In this context, the feedback on the implementation of the Compliance Officer function undoubtedly offers some interesting avenues for the

[79] However, the function of Compliance Officer now extends to other areas, such as competition and the environment.

[80] On this role of "facilitator", see namely K. Rosier « Délégué à la protection des données: une nouvelle fonction, un métier en devenir », *op. cit.*, p. 136. See also WP29, Guidelines on Data Protection Officers ('DPOs'), 16/ENWP 243 rev.01, Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, p. 5.

[81] Article 39(1)(e) of the GDPR.

[82] In doing so, the strengthening of the role of the DPO nevertheless echoes the proposal of the French Council of State to introduce a right of reporting with regard to data protection (Conseil d'État français, Rapport 2014: « Le numérique et les droits fondamentaux », Proposition n° 7, p. 282).

[83] In the context of this obligation, Jeroen Terstegge qualifies *expressis verbis* the DPO as a "whistleblower" ("EU Watch: Data protection and the new face of privacy compliance", *Business Compliance*, 2013, n° 6, p. 40). In this sense, see also R. de Quenaudon, « Les lanceurs d'alerte » *in Prendre la responsabilité au sérieux* (A. Supiot & M. Delmas-Marty, eds), Paris, P.U.F., 2015, p. 303.

[84] Article 38(3) of the GDPR.

[85] Article 39(1)(d) of the GDPR.

[86] Article 38(3) of the GDPR. About the protection of the DPO against reprisals, see namely K. Rosier, « Délégué à la protection des données: une fonction multifacette » *in Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie* (C. de Terwangne & K. Rosier, eds), 1ère éd., coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 582-583.

construction of both the Data Protection Officer and Whistleblower Officer functions[87].

B. The Open Door to Whistleblowing

The logic of whistleblowing may be derived from data protection rules in themselves. Article 38(4) of the GDPR states that "data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation". Moreover, the DPO needs information to exercise his tasks, in particular of reporting to the highest level of management.

Such provision does not necessarily imply the establishment of whistleblowing mechanisms. However, practice notes that "more and more companies believe that it is in their interest to ensure that whistleblowers can find a sympathetic ear internally and are not forced to turn to the general public"[88].

In any event, data protection reporting systems must now be established under the Directive on whistleblowers. The Directive emphasises in this respect that "[r]espect for privacy and protection of personal data, which are enshrined as fundamental rights in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the 'Charter'), are other areas in which whistleblowers can help to disclose breaches, which can harm the public interest"[89].

It follows that the reporting mechanisms established under the Directive on whistleblowers should also apply to "personal data breaches" within the meaning of the GDPR, i.e. "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[90]. The controller must indeed necessarily be aware of personal data breaches that take place in order to comply with the obligation to notify the supervisory authority established by Article 33(1) of the GDPR[91].

---

[87] J. Terstegge, *op. cit.*, p. 40.

[88] In French, read: companies are "de plus en plus nombreuses à penser qu'il est de leur intérêt de veiller à ce que [les] lanceurs d'alerte puissent trouver une oreille attentive en interne et ne soient pas contraints de se tourner vers le grand public" (F. Coton & J.-F. Henrotte, « Affaire Cambridge Analytica: les quatre enseignements à retenir pour un DPO », *DPO news*, 2019, n° 2, p. 11).

[89] Recital 14 of the Directive on whistleblowers.

[90] Article 4(12) of the GDPR.

[91] "In the case of a personal data breach, the controller shall, in accordance with Article 33 of the GDPR, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority

In the same order, the European Parliament legislative resolution of 16 April 2019 notes that "[s]imilar considerations apply for breaches of the Directive on the security of network and information systems, which introduces notification of incidents (including those that do not compromise personal data) and security requirements for entities providing essential services across many sectors (e.g. energy, health, transport, banking, etc.) for providers of key digital services (e.g. cloud computing services) and for suppliers of basic utilities, such as water, electricity and gas. Whistleblowers' reporting in this area is particularly valuable in order to prevent security incidents that would affect key economic and social activities and widely used digital services, as well as to prevent any infringement of Union data protection legislation"[92].

In the light of those considerations, it must be accepted that a worker who expresses data protection concerns to the DPO, even if those concerns do not concern him or her directly, should enjoy the protection offered by the Directive on whistleblowers if he or she has complied with the conditions laid down by that directive.

With regard to the Directive on whistleblowers, it should even be accepted for an employee to notify breaches of personal data directly to the supervisory authority (external reporting)[93].

With this in mind, Mark Zuckerberg's company decided, in the context of the *Cambridge Analytica* case, to create a "Data Abuse Bounty Program" to help protect its users' data from security breaches and abuses[94]. Such a system aims to contain reports at company level, filtering at the same time reports that may reach public authorities.

---

competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay".

[92] Recital 14 of the European Parliament legislative resolution of 16 April 2019 on the proposal for a directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law (COM(2018)0218 – C8-0159/2018 – 2018/0106(COD)).

[93] In the United Kingdom, the notification of security breaches to the supervisory authority has been spontaneously examined as a whistleblowing scheme (see namely R. BREAVINGTON, « GDPR introduction sees whistle-blower reports on data breaches rise 165 % », *Lexology.com* (accessed December 18, 2018)). The ICO, the British DPA, receives disclosures from whistleblowers pursuant to the Public Interest Disclosure Act of 1998. See https://ico.org.uk/about-the-ico/our-information/whistleblowing-disclosures (accessed November 25, 2020).

[94] *Data Abuse Bounty Program*, Q/A, available at www.facebook.com (accessed April 12, 2018).

Conclusion

Since the end of the 1970s, the human mania for denunciation, sometimes exalted, sometimes enclosed, has taken on a new face thanks to the galloping phenomenon of whistleblowers.

For a long time, the sole purpose of "denunciation", understood as the reporting of a criminal act to an administrative or judicial police officer[95], was to attract the favors of a prince protector. Today it is distinguished by the pursuit of a resolutely new purpose, closely linked to the recognition of individual rights and freedoms at the end of the Second World War, the defense of the public interest. Freely and conscientiously, the whistleblower speaks up against irregularities committed by private and public powers because silence has become an alternative, where for a long time it was a condition for survival.

In this evolution, ICTs are playing a substantial role, reshaping the human practice of "denunciation" at two levels. At the level of the operation itself first, ICTs greatly facilitate the whistleblower's information gathering work but also the work of data analysis by recipients, especially journalists. Secondly, at the level of the legitimacy of the operation, ICTs allow for the whistleblower to easily substantiate his or her allegations, where the informer had to or could formerly be satisfied with rumors. Moreover, whistleblowing may be seen as a bulwark to thwart the actions of a "Big Brother" in the making.

While the new phenomenon of whistleblowers has been completely ignored by the GDPR, it must be noted that the Directive on whistleblowers, for its part, has by no means ignored the European data protection regulation.

The implementation of whistleblowing through the data protection filter certainly participates to the acculturation process followed by the Anglo-American institution of whistleblowing in Europe.

This is a welcome step, as EU data protection rules make it possible both to combat unjustified alerts and to support justified alerts, especially when these alerts concern issues that affect the right to privacy and data protection.

[95] See namely G. Cornu (eds.), *Vocabulaire juridique*, Association Henri Capitant, 8e éd., Paris, P.U.F., 2000, p. 274; R. Merle & A. Vitu, *Traité de droit criminel*, Paris, Cujas, 1967, p. 833; A. Chauveau & F. Hélie, *Théorie du Code pénal*, Tome II, 2e éd., Bruxelles, Bruylant-Christophe et compagnie, 1865, p. 209, n° 3099.