The directive on whistleblowers to the test of the digital society

Kafteranis, Dimitrios; Lachapelle, Amelie

Published in:
Time to reshape the digital society

Publication date:
2021

Document Version
le PDF de l'éditeur

CHAPTER 1
The directive on whistleblowers to the test of the digital society: Between hope and desillusion

Dimitrios KAFTERANIS[1] **& Amélie LACHAPELLE**[2]

Introduction

1. If some people still had doubts about the value of alerting of malpractices in the digital technology field, Frances Haugen's recent revelations about Facebook are a good reminder. The whistleblower reveals, among other things, how the social network feeds misinformation online and encourages its users' dependence on its services. When it comes to the trade-off between increased profits and user welfare, the balance is always tipped in favour of increased profits.

This is all the more alarming that Facebook, as noted by Vigjilenca Abazi and Helen Todd, "has much more power than should be in private hands"[3]. This private company – bigger than any country if we base on the number of people[4] – has even to some extent more power than a state or an international organization like European Union. This is a core issue.

However, it is not at all clear that such revelations are covered by the EU Directive on whistleblowers.

---

[1] Doctor of Legal Sciences. Assistant Professor in Law, Centre for Financial and Corporate Integrity, Coventry University.

[2] Doctor of Legal Sciences. Senior Lecturer at the UNamur and Senior Researcher at the CRIDS/NaDI.

[3] V. ABAZI & H. TODD, "Dethroning Facebook's Benevolent Dictator", *Techonomy*, online, 18 June 2021 (last access on 6th October 2021).

[4] Vigjilenca Abazi and Helen Todd highlight than "simply based on the number of people, Facebook is the largest group in the world, far bigger than any country, with 3.1 billion people logging in monthly across its core family of apps". See V. ABAZI & H. TODD, *ibid*.

2. On October 2019, the European Union adopted the Directive 2019/1937 on the protection of persons who report breaches of Union law ("Directive" or "DWB" hereinafter). The long-awaited Directives comes, partially, as an answer to the several scandals that shaked the European and international society, the uneven protection of whistle-blowers in several Member States and the work of the European Parliament towards its adoption. From the limelight to the light, whistleblowers are now part of the EU legal order and common minimum requirements are available across the EU. The Directive has several "innovative" elements but also drawbacks that may affect whistleblowers' protection in the near future.

In the Information and Communication Technologies' ("ICTs" hereinafter) area, the Directive puts the focus on privacy, data protection and cybersecurity. Even if those three areas are explicitly covered by the Directive, it is however doubtful that the disclosures made in these areas are all protected by the Directive: on the one hand, because the Directive shall only apply to persons working in the private or public sector who acquired information on breaches in a work-related context[5]; on the other hand, because the Directive shall only apply to breaches falling within the scope of the Union acts set out in an Annex[6].

While there is no shortage of examples – Snowden, Cambridge Analytica, Pegasus, etc. – to demonstrate the urgent need to protect people who warn of the risks posed by today's technologies – whether they tend to stimulate the purchase of goods, monitor our actions, direct our vote or ideas, usurp our identity or steal our data – it is clear that the legal framework remains far below what is required. Would Edward Snowden, Brittany Kaiser, Frances Haugen, … and co be protected by the Directive? What about the ethical hackers who blow the whistle?

Furthermore, it should be noted that "ethical hackers" (also called "white-hat" hackers) remain totally ignored by the European legislator (as well as the Belgian legislator). Nonetheless, the latter play an important role in the field of cybersecurity by identifying, as a proper "vulnerability finder" the vulnerabilities of the information networks and information systems submitted to their evaluation. They are also and above all "potential whistleblowers". If the response of the entity they are screening does not seem adequate and the lack of response is likely to threaten the public interest, they may well decide to blow the whistle. Similarly, by penetrating an information system or network, they may become aware of information about illegal or abusive acts that should be reported or revealed publicly under the DWB.

[5] Article 4 of the DWB.
[6] Article 2 of the DWB.

3. The objective of this paper is to propose a first study of the main issues arising from the application of the Directive in the digital era. In particular, we address two questions.

First point concerns the material scope of the Directive (II). Is it broad enough to cover all the risks posed by ICTs?

Given the role played by ethical hackers in the field of cybersecurity, it is surprising that the EU lawmaker completely ignored their existence when adopting the DWB (III). Could an ethical hacker benefit from whistleblower protection? Could an ethical hacker use whistleblowing channels?

Before considering these two issues, we explain why we need to take seriously whistleblowers in the technological area (I).

I. Why do we need to take seriously persons who blow the whistle in the digital technology area?

A. The need to ensure security of networks and information systems

4. Cyber-attacks are a growing threat to businesses and governments.

The problem with cyber warfare is that we don't see it as such. It is invisible. Yet its effects are very visible. The presidential election of Donald Trump has shown us this. The former American president owes his election not only to the exploitation of the Facebook data of American voters by the company Cambridge Analytica, but investigations in the United States have shown that the Russian intelligence services had carried out cyber operations on the American electoral system[7]. In this case, voter lists and vote counts were not altered, but what if they had been? There is a real risk that a group of hackers could penetrate the electoral system of another state in order to manipulate the ballot. This group could act autonomously or on behalf of an enemy state.

Cyber-attacks can also lead to loss of life. And that is why the security of critical infrastructure information systems and networks is receiving so much attention. What would happen if the switch system of a railway line was attacked? The electrical generators of a hospital? The power generation system of a nuclear power plant?

[7] K. Harris, *Nos vérités. Mon rêve américain*, Paris, Robert Laffont, 2021, pp. 262-263.

Without jeopardising our democratic system or threatening human life, cyber-attacks can also paralyse the economic system. They can alter the supply chain, order forms, the provision of services or the manufacture of products by one or more companies. These risks will increase as digital technology becomes more important in the business model of companies (use of drones, driverless cars, automatic order forms, data sensors, etc.).

These cyber-attacks also threaten users' right to privacy and data protection in that they can take the form of data leakage or data theft.

5. Currently, the main problem is that the technologies developed are not as effective as they should be and it is not possible for those who acquire these technologies to verify their effectiveness before an attack actually takes place[8].

Many business owners and many administrations buy software and then keep their fingers crossed that nothing goes wrong. Unless you are an expert in cyber security – and even then – it is difficult to predict whether a piece of software will be able to guarantee the security of your infrastructure and your network. It is only when an attack is thwarted that the company is able to say whether the choice of software was appropriate or a bad idea.

Hence the idea of using "geeks" for whom hacking is a game. Ethical hackers or white-hat hackers allow companies and governments to monitor the resilience of their computer systems before an attack occurs.

But if the company or the government get a nasty surprise from ethical hacking, they may still want to cover up the revelations. The ethical hacker must be able to blow the whistle, and in so doing benefit from the status of whistle-blower, without risking prosecution for hacking. By disclosing the incident for the benefit of stakeholders, whistleblowers push organisations to raise their cybersecurity standards.

Besides these white-hat hackers, directly employed by a company, there are others who are not employed by a company but, out of activism, conduct unsolicited hacks in order to disclose the vulnerabilities of public or private network systems to the public.

However, the DWB on whistleblowers totally ignores the practice of "ethical" or "white-hat" hacking. An "ethical hacker" could be qualified for protection as a "whistle-blower"?

[8] Debate Security, Research Report: Cybersecurity Technology Efficacy: Is cybersecurity the new market for lemons?, October 2020.

B. The need to have watchdogs in the digital environment to ensure the respect for human rights

6. As the NIS Directive recalls in its first recital, "network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market". More broadly, the recent pandemic has showed that all the functioning of our modern societies depends on network and information systems. This is a consequence of the digital era.

Nevertheless, the ICTs represent a significant threat to individual freedoms. One spontaneously thinks about privacy and freedom of expression, but other fundamental rights are threatened, such as the right to health, the right to live or the right to free elections.

The regulation of ICTs as a threat to individual freedoms in Europe is based on two sets of texts: the first relates to privacy and data protection and the second to cybersecurity.

Both the governance system set up by the GDPR and the one set up by the NIS Directive totally ignore whistleblowers.

However, their role in the field of privacy, data protection and cybersecurity should not be overlooked. There are enough recent cases – Snowden case, Cambridge Analytica Files, Pegasus case – to remind us of this. The European lawmaker rightly included this area among those covered by the DWB. An infringement of EU law in this area is likely to cause serious harm to the public interest. According to Michaël Bardin, the asymmetry of information, which has reached enormous proportions today, is the basis for the legitimacy of whistleblowers in the digital area[9]. Whistleblowing aims to rebalance the relationship between the holder of information deemed important, such as a state organisation (*e.g.* NSA) or a company (*e.g.* Facebook) and others.

7. If Facebook has as much power as a state, it should at least be subject to the same democratic control. This control should even be strengthened since it was not elected by the people and yet it rules them without the people noticing[10].

---

[9] M. Bardin, «Les "lanceurs d'alerte" à l'ère du numérique: un progrès pour la démocratie?», in O. de David Beauregard-Berthier & A. Taleb-Karlsson (coord.), *Protection des données personnelles et Sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique?*, Bruxelles, Bruylant, 2017, pp. 252-253.

[10] This is one reason why Vigjilenca Abazi and Helen Todd speak about a "dictator" in a recent paper. See V. Abazi & H. Todd, "Dethroning Facebook's Benevolent Dictator", *Techonomy*, online, 18 June 2021 (last access on 6th October 2021).

The recognition of fundamental rights and freedoms aims a purpose of empowerment. In the traditional approach, individuals are understood as acting as citizens rather than as subjects. In the modern approach, born in the digital context, individuals are understood as acting as citizens rather than as products. The right to informational self-determination, recognised by the European Court of Human Rights under Article 8 of the Convention, pursues such an objective. When this right is breached, which happens often, we must be able to speak up.

II. Is the "technological risk" totally covered by the scope of the Directive?

8. Article 2.1 of the DWB states:

> "This Directive lays down common minimum standards for the protection of persons reporting the following breaches of Union law:
> (a) breaches falling within the scope of the Union acts set out in the Annex that concern the following areas:
> […]
> (x) protection of privacy and personal data, and security of network and information systems;
> […]"

Regarding the area "protection of privacy and personal data, and security of network and information Systems", the Annex mentions the three following Union acts:

> "(i) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37);
> (ii) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1);
> (iii) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1)."

This means that, in the technological area, the DWB shall protect three types of breaches:

i) Breaches of the e-privacy Directive[11]

ii) Breaches of GDPR

iii) Breaches of NIS Directive

Under Article 5 of the Directive, "'breaches' mean acts or omissions that are unlawful and relate to the Union acts and areas falling within the material scope referred above or defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope referred above.

A. Reporting channels in the privacy, data protection and cybersecurity area

9. The mentioned Union acts already establish reporting channels, but these were not designed for whistleblowers.

Pursuant to Article 33.1 of the GDPR, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify any personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Pursuant to Article 34.1 of the GDPR, the controller shall also communicate the personal data breach to the data subject without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons,

Under Article 4(12) of the GDPR, data breach "means 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".

Moreover, it should be noted that 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". While the GDPR doesn't expressly mention reports from whistleblowers, it is obvious that the DPO is, at first glance, the most appropriate person to receive reports about infringement of the GDPR, a fortiori when the data controller has not formerly put in

[11] It should be noted that a new regulation – "e-privacy regulation" – to repeal and replace the directive is currently being negotiated at the European level.

place whistleblowing channels. The only limit – but essential limit – is to ensure that this task does not lead to a conflict of interest[12].

Where appropriate, the DPO will be able to blow the whistle to the highest management level of the controller or the processor, but also to the data protection authority.

Pursuant to Article 14.3 of the NIS Directive, "the operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide". Pursuant to Article 16.3 of the NIS Directive, "the digital service providers likewise notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III [of the Directive] that they offer within the Union". The operators of essential services and the digital service providers have to take upstream appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use[13].

Under Article 4(7) of the NIS Directive, an incident is "any event having an actual adverse effect on the security of network and information systems".

A "security incident" can result in personal data breaches. In this hypothesis, both reporting duties shall apply.

According to the same logic of the one in the Article 34.1 of the GDPR, Article 4.2 of the e-privacy Directive provides that "in case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved".

Recital 20 of the e-privacy Directive indicates that "security is appraised in the light of [Article 32 of the GDPR]"[14].

The e-privacy Directive doesn't define the concept of "risk of a breach of the security of the network" nor the concept of "breach of the security of the network", but it appears from Recital 20 of the e-privacy Directive that they can be understood in the light of the concept of "data breach"

[12] Article 38.6 of the GDPR; Recital 56 of the DWB. About this topic, see namely A. Lachapelle, "Data protection enforcement in the era of the Directive on whistleblowers: towards a collective approach?", in E. Kosta & R. Leenes (eds), *Research Handbook on EU Data Protection Law*, Cheltenham, Edward Elgar Publishing, 2022.

[13] Article 14.1 and 16.1 of the NIS Directive.

[14] Recital 20 of the Directive e-privacy refers to Article 17 of the former Directive 95/46/EC.

as defined in the GDPR. The concept of "security risk" can be understood in the light of the concept of "risk" as defined in the NIS Directive.

B. The whistleblower, a vital link in the risk management policies

10. How can an entity be aware of a data breach, an incident or a security breach? Whistleblowers can clearly help them to detect security incidents and data breaches.

In this sense, Recital 14 of the DWB reads as follows:

> "Respect 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. Whistleblowers can also help disclose breaches of Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of network and information systems, which introduces a requirement to provide notification of incidents, including those that do not compromise personal data, and security requirements for entities providing essential services across many sectors, for example energy, health, transport and banking, for providers of key digital services, for example cloud computing services, and for suppliers of basic utilities, such as water, electricity and gas. Whistleblowers' reporting in this area is particularly valuable for the prevention of security incidents that would affect key economic and social activities and widely used digital services, as well as for the prevention of any infringement of Union data protection rules. Such reporting helps ensure the continuity of services that are essential for the functioning of the internal market and the wellbeing of society".

Does this mean that whistleblowers qualify for protection under the DBW when they report a "data breach", a "security breach" or an "security incident"?

We can state that a "data breach" is a breach under the DWB. Considering that a breach of security is a breach of security requirements provided by GDPR, we can also assume that a "security breach" is a breach within the meaning of the DBW.

This is not so clear regarding the reporting of an "incident" under the NIS Directive. Indeed, under Article 4(7) of the NIS Directive, an incident

is "any *event*[15] having an actual adverse effect on the security of network and information systems".

The same concerns apply to "security risk" under the NIS Directive knowing that under Article 4(9) of the NIS Directive, risk "means any reasonably identifiable *circumstance or event*[16] having a potential adverse effect on the security of network and information systems". In this regard, similar concerns could be raised concerning the "risk of a breach of the security of the network" under the e-privacy Directive.

Currently, it is not obvious that an "event" is an unlawful or abusive act or omission. Accordingly, it is not obvious that a security incident or a security risk is a breach under the DWB.

While whistleblowing mechanisms are an appropriate and organisational measure to manage the (technological) risks and to handle both the incidents and the data breaches, it is thus not sure that they will be entitled for protection in this framework, except in the case of a data breach reporting.

This concern has not to be taken lightly. Since the DWB is innovative, the national judge can be expected to give it a literal reading or at least a strict interpretation.

We can make those observations in any area covered by the DWB, but they seem even more surprising in areas such as data protection and cybersecurity, governed by legislation that incorporates a risk-based approach[17].

Furthermore, it must be noted that whistleblowing, in its French meaning of "ethical alert", is defined as "a personal or collective approach aimed at mobilizing authorities supposed capable of acting and, at least, informing the public of a danger, the imminence of a disaster, the uncertain nature of an enterprise or a technological choice"[18].

As defined at the EU level, whistleblowing should necessarily attempt to reconcile the French approach and Anglo-American approaches of whistleblowing. Besides, Francis Chateauraynaud and Didier Torny

[15] We underline.

[16] We underline.

[17] On the risk-based approach in cybersecurity, see namely J.-N. Colin, "Risk as the Cornerstone of Information Security and Data Protection", in J. Herveg (ed.), *Deep diving into data protection*, Bruxelles, Larcier, 2021, pp. 255-270.

[18] In French, you can read: "une démarche, personnelle ou collective, visant à mobiliser des instances supposées capables d'agir et, pour le moins, d'informer le public d'un danger, de l'imminence d'une catastrophe, du caractère incertain d'une entreprise ou d'un choix technologique" (F. Chateauraynaud & D. Torny, *Les sombres précurseurs. Une sociologie pragmatique de l'alerte et du risque*, 2e éd., Paris, EHESS, 2013, p. 37).

rightly address the status of "lanceur d'alerte" as the meeting together of two reporting logics, that of the denunciation (reporting of a person) and that of the alert (reporting a risk or a danger)'[19]. Under this approach, "whistleblower" is a potential "informer" in a positive sense.

C. The Union acts mentioned in the Annex of the DWB

11. Finally, the list set out in the Annex seems to be shorter too considering the relevant legislation in the area of privacy, data protection and cybersecurity.

Concerning the privacy and data protection area, we are surprised not to see mentioned the Directive (EU) 2016/680 and the Regulation (EU) 2018/1725. It must be said that the DWB actually does not apply to persons working within Union institutions, bodies, offices or agencies[20]. Those entities are only considered as potential competent authorities.

Concerning the cybersecurity area, it should be acknowledged that the list is too short in so far as it only mentions the NIS Directive[21]. What about the specific security requirements[22] laid down in the Directive 2002/21/EC of the European Parliament and of the Council[23] and in the Regulation (EU) No 910/2014 of the European Parliament and of the Council[24]?

Are revelations of the Pegasus Project covered by the Directive? Obviously not. The Pegasus Project has, however, shown that it is useful to monitor the use of privately developed surveillance software by governments. Diverting surveillance software from its contractual purpose (in this case, using the software not only to prevent serious crimes such as

---

[19] In French, you can read: "un cas particulier de rencontre entre deux logiques de signalement, celle de la dénonciation (signalement d'une personne) et celle de l'alerte (signalement d'un risque ou d'un danger)" (F. Chateauraynaud & D. Torny, *ibid.*, p. 21).

[20] D. Kafteranis, "A new enforcement tool: a Directive to protect whistle-blowers", *Business Law Review*, n° 41, 2020, p. 50.

[21] For an overview of the relevant legislation, see namely A. Cruquenaire, "La cybersécurité, un enjeu à la croisée des stratégies européennes", in *Liber Amicorum Denis Philippe*, 2022, under press.

[22] Both regulations are excluded from the application of the NIS Directive (article 1.3 of the NIS Directive and Recital 7).

[23] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), *O.J.*, L 108, 24 April 2002, p. 33.

[24] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *O.J.*, L 257, 28 August 2014, p. 73.

terrorism, but also to monitor political dissidents) does not a priori violate any cybersecurity rules, even if it obviously undermines the cybersecurity of the individuals under surveillance.

More broadly, it is doubtful that compliance with data protection and cybersecurity laws will be sufficient to address the "technology issue".

12. Having regard to the foregoing, the DWB could (should) have gone further.

It must be concluded that in its current state, the DWB does not totally participate in the enforcement of the e-privacy Directive, of the GDPR and of the NIS Directive. Moreover, it does really not cover the "technological issue". Too many gaps remain, which may discourage potential whistleblowers, especially since the personal scope of the DWB is also not without criticism.

If we take recent cases mentioned before, it is not sure that reporting the misuse of surveillance software from its contractual purpose, as in the Pegasus case, is protected by the DWB. Nor is it certain that the facts exposed by Edward Snowden would have fallen under the scope of the DWB, even if the massive surveillance activities in question had been carried out by European governments. Indeed, the Directive (EU) 2016/680 falls outside the scope of the DBW, as everything related to intelligence, defense and domestic security by the way, which remain under the discretionary power of the States.

III. Are all the potential whistleblowers in digital technology matters covered by the Directive?

13. The other question we address in this paper is to see if the "digital technology whistleblowers" are totally covered by the personal scope of application of the DWB, and in particular the potential whistleblowers in cybersecurity matters. The "ethical hacker" is a potential digital technology whistleblower for the reasons explained above in the introduction.

Article 4 of the DWB states:

> "This Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following:
> (a) persons having the status of worker, within the meaning of Article 45(1) TFEU, including civil servants;

(b) persons having self-employed status, within the meaning of Article 49 TFEU;
(c) shareholders and persons belonging to the administrative, management or supervisory body of an undertaking,
including non-executive members, as well as volunteers and paid or unpaid trainees;
(d) any persons working under the supervision and direction of contractors, subcontractors and suppliers.
2. This Directive shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended.
4. The measures for the protection of reporting persons set out in Chapter VI shall also apply, where relevant, to:
(a) facilitators;
(b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and
(c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context."

A. The work-related context

14. The definition of the whistle-blower, under the DWB, is large entailing employees from the public and private sector. These employees can be actual employees, ex-employees, persons in the recruitment phase, volunteers, trainees, contractors and others, creating a large meaning of the term "employee".

As can be seen, the whole personal scope revolves around the work-related context. This is this work-related context which justifies the setting out of a specific legal protection. Indeed, persons which acquire the information they report through their work-related activities "run the risk of work-related retaliation, for instance, for breaching the duty of confidentiality or loyalty. The underlying reason for providing such persons with protection is their position of economic vulnerability vis-à-vis the person on whom de facto they depend for work. Where there is no such work-related power imbalance, for instance in the case of ordinary complainants or citizen bystanders, there is no need for protection against retaliation"[25].

[25] Recital 36 of the Directive.

15. If we take the example of Edward Snowden, Brittany Kaiser and Frances Haugen, the personal scope of the DWB is broad enough to protect them.

But what about the ethical hackers?

We can state that ethical hackers can fulfil the role of whistleblowers and this novel function is illustrated by the rise of cybersecurity whistleblowers[26]. Cybersecurity whistleblowers came into the limelight due to significant incidents such as the Equifax breach, WannaCry ransomware and the Cambridge Analytica[27].

The ethical hacker, potential whistleblower, doesn't usually act in a professional context. Actually, he rarely does so when he is acting like a whistleblower, since his job is limited to testing a network or information system for possible vulnerabilities and reporting them to the company concerned. The ethical hacker is not "supposed" to act as a whistleblower. However, once the door has been opened, his expertise enables him to discover many things and his ethics may lead him to want to blow the whistle… Another hypothesis could be that the ethical hacker would like to "check" a few months after his first intrusion if the enterprise has taken into consideration his report and, where appropriate, to blow the whistle. This "checking" goes beyond the coordinated vulnerability disclosure policies[28] without stopping to strengthen enforcement of cybersecurity rules.

It is clear that the ethical hacker is clearly not an "ordinary complainant" or a "citizen bystander". Conversely, for sure he runs the risk of serious retaliation. However, it is really questionable whether he will be protected by the Directive as implemented by the Member States. This protection is, however, very helpful since the activity of ethical hacking is, as a rule, unlawful without an authorization from the entity tested and that even if the white-hat hacker has the best of intentions[29].

---

[26] D. Hammer & E. Bundschuh, "The Rise of Cybersecurity Whistleblowing", *Compliance & Enforcement*, 29th December 2016, available at: https://wp.nyu.edu/compliance_enforcement/2016/12/29/the-rise-of-cybersecurity-whistleblowing/ (last access on 6th October 2021)

[27] See namely "Cybersecurity threatscape: Q2 2018", *Positive Technologies*, 2 October 2018, https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q2/ (last access on 6 October 2021).

[28] The "coordinated vulnerability disclosure" (CVD) "is a process where vulnerability finders work with either vendors or coordinators to minimise the risk of an identified vulnerability and typically involves a set of steps that require careful management so as to avoid potential negative impacts, which otherwise could be substantial" (ENISA, *Economics of vulnerability disclosure*, December 2018, p. 12).

[29] In the case of a company, the situation is the following: companies where security problems are identified, may decide to cover up the problem by deleting information or silencing incidents. In this kind of situations, ethical hackers are in a delicate position as they

Laws in the field such as the UK's Computer Misuse Act 1990 and the US's Computer Fraud and Abuse Act 1984 do not recognize the concept of ethical hacking. This means that the ethical hacker can easily be prosecuted for breaching these laws. For instance, due to the sensitive nature of the information, it is highly possible that a trade secrets violation may occur[30]. Ethical hacking is a notion that does not exist under criminal law. Prosecutors, often, should rely on the notion of good faith or bad faith in order to distinguish between white and black hat ethical hackers and, finally, decide whether to prosecute or not. As the motives of whistleblowers tend to fade out in the assessment of their protection, it would be opportune to examine the proportionality of the hacker's actions[31]. This proportionality check will be necessary to check if the hacker has done what was needed to expose the breach. Despite the usefulness of a proportionality test, this is not always possible and there are difficulties such as the impossibility for the ethical hacker to predict in advance what will render the examination of motives relevant even in future whistleblowing cases[32].

B. The motivation of the reporting person

16. Under Article 6.1 of the DWB, whistleblowers shall qualify for protection provided that: (a) they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this Directive; and (b) they reported either internally or externally in accordance with the procedure established under the Directive, or made a public disclosure in accordance with Article 15.

The employee can report either internally or to the competent authorities without any prior obligation to report internally at first. This freedom of choice for the disclosure channels for whistleblowers is a significant innovation of the Directive. In addition, the Directive aims to protect whistleblowers from retaliation, and to neutralise civil, administrative

---

are the ones who brought the "bad news" and they may face reprisals in the form of job termination or legal action against them. Outdated laws are a fertile ground against ethical hackers, especially in the field of criminal law.

[30] M. J. Pacella, "The Cybersecurity Threat: Compliance and the Role of Whistleblowers", *11 Brook J Corp Fin and Com L 39*, 2016, pp. 49-50.

[31] K. Pender, S. Cherkasova & A. Yamaoka-Enkerlin, "Compliance and Whistleblowing: How Technology Will Replace, Empower and Change Whistleblowers", in J. Madir (ed.), *Fintech – Law and Regulation* 2019, pp. 326-352.

[32] K. Pender e.a., *ibid*.

and criminal liability. These elements are important steps towards achieving a more effective protection of whistleblowers at the EU level.

17. Unlike the European Court of Human Rights, the European lawmaker therefore decided to remove the criteria of the motivation. According to Recital 32 in fine, "the motives of the reporting persons in reporting should be irrelevant in deciding whether they should receive protection". In any way, it is obvious that the malicious hacker – so called "black hat" – is for hacking what the snitch is to reporting. In the same way, the ethical hacker – so called "white hat" – is for hacking what the whistleblower is to reporting. By definition, the ethical hacker "is a person with good intentions who, with the consent of the responsible organisation, wishes to contribute to a better security of the information systems. He can, for example, carry out pen tests or use other methods to check the security of information systems. He is in direct opposition to the hacker who uses his skills to gain unauthorised access to a system with bad intentions. The participant should inform the person in charge of the information system or a coordinator of any vulnerabilities discovered, so that they can be eliminated"[33].

C. The granting of a bounty

18. A last issue should be addressed regarding ethical hacking. According to Recital 30, the Directive "should not apply to cases in which persons who, having given their informed consent, have been identified as informants or registered as such in databases managed by authorities appointed at national level, such as customs authorities, and report breaches to enforcement authorities, in return for reward or compensation".

May the ethical hacker who is receiving a bounty be qualified for protection under the Directive?

"Bug Bounty Programs" are frequent in practice. A Bug Bounty Program (also known as Vulnerability Rewards Program) is a form of coordinated vulnerability disclosure policy, which allows organisations to provide a reward for the "participant" or "vulnerability finder", depending on the number, importance or quality of the vulnerability information provided.

[33] FAQ on coordinated vulnerability disclosure policy (CVDP) and bug bounty programmes: What is a CVDP participant or "ethical hacker"?, https://ccb.belgium.be (last access on 6th October 2021).

The bounty can be in the form of money, gifts or public recognition (ranking among the best participants, publication, conference, etc.)[34].

Insofar as the reward is granted by the company implementing the coordinated vulnerability disclosure policy, we believe that it should not be an obstacle to the application of the whistleblowers' protection under the DWB.

Conclusion

19. The adoption of the EU Directive is a positive step towards the legal protection of whistleblowers in the EU. The whistleblower now has specific rights, obligations and protection under EU law. Nevertheless, the Directive fails to consider carefully whistleblowers working in the digital technology sector and largely ignores the technology itself. The pace of developments in the technology sector is fast, problems and issues are created and new solutions to these problems and issues should be given. There is an inherent need for information. This information can be given by whistleblowers. These employees are either whistleblowers or white-hat hackers who are ready to provide information (whistleblowers) or to test the security of network systems (ethical hackers). They have minor differences but the same goal: report breaches that affect their company, society or the economy. Their work is important and, as a result, their status should become clearer under current legislation and their protection as well.

One can fear that protection of whistleblowers raises risks of widespread surveillance when we are just trying to protect ourselves from this surveillance. Recent widely reported cases are, however, enough to reassure.

20. In the digital era, whistleblowing has become a categorical imperative for fighting against the mass governance and surveillance. Edward Snowden, Brittany Kaiser, Frances Haugen and all the others whistleblowers[35] have taken risks in order to make us free.

Whistleblowers do not build our chains but, instead, break them up.

---

[34] See namely CCB, *Les politiques de divulgation coordonnée des vulnérabilités. Coordinated Vulnerability Disclosure Policy*, Brochure, 2020, p. 4; V. Vander Geeten, «La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités», in F. Dumortier & V. Vander Geeten (eds), *Les obligations légales de cybersécurité et de notifications d'incidents*, Bruxelles, Politeia, 2019, pp. 217-265.

[35] It is obvious that the Pegasus case can be exposed thanks to the help of insiders, but their identity is not known.