Getting Whistleblower Protection Right:

A Practical Guide to Transposing the EU Directive

Authors:
Naomi Colvin, Bruno Galizzi and Veronika Nad

blueprint for FREE SPEECH

E.A.T. EXPANDING ANONYMOUS TIPPING

Acknowledgements

Blueprint for Free Speech gratefully acknowledges the support of the Open Society Initiative for Europe within the Open Society Foundations. The Expanding Anonymous Tipping (E.A.T.) Project also gratefully acknowledges the Internal Security Fund of the European Union.

We thank Professor David Lewis of Middlesex University, Tom Devine and Samantha Feinstein of the Government Accountability Project (GAP), Katharina Beck, Robert Benditz, Isabelle Brams, Adrien Giraud, Peter Neuboeck, and Sven Voelcker of Latham & Watkins LLP for their valuable insights and reviews.

Co-funded by the Internal Security Fund of the European Union

This report was partly funded by the European Union's Internal Security Fund — Police. Its content represents the views of the authors only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

blueprint for FREE SPEECH

TABLE OF CONTENTS

Introduction

Many of the major news stories of the last decade have involved a whistleblower at some point along the line. Whether we're talking about the undemocratic influence of online political advertising, large-scale international tax fraud or the neglect of environmental and public health evidence exposed in the so-called Dieselgate scandal, our public debate would be much poorer without the contribution of whistleblowers.

It will likely take decades to determine the full range of damage that was mitigated, or prevented, by these issues coming to light. But there can be no doubt that without the contribution of those who made the choice to speak up, the costs incurred to society would have been significantly larger.

Whistleblowers are human early warning systems detecting anything from simple mistakes and related cover-ups to systematic abuse and fraud affecting entire societies. Their actions not only help to prevent severe damage, but also contribute to improved global business ethics and a general culture of transparency, the value of which has become even more obvious in the context of battling the global COVID-19 pandemic.

Yet coming forward with information is a risky business and this remains the case whether whistleblowers try to report to their employers - as over 90% of them do -, go straight to a regulator or, less often, to the media. Retaliation can mean suffering damage to career prospects or being out of a job entirely, incurring significant financial costs. Fighting to be recognised and compensated as a whistleblower can itself become a full-time job. Too many whistleblowers end up in lengthy and expensive court battles, even when they are trying to enforce rights that are meant to protect them[i].

These risks are well understood by those who have information to share. Surveys regularly find that those who witness wrongdoing are deterred from coming forward because they fear reprisal and do not believe that there are effective systems to prevent this from happening[1].

If we want whistleblowers to come forward, to act as an early warning system in the organisations they know and to raise the alarm about genuinely serious instances of wrongdoing, then we need to make sure that making a report does not become a life-changing event. Introducing legal protections are one way of doing that.

Whistleblower protection laws aim to regularise practice in a challenging area, to ensure that concerns are investigated and limit the risks to all parties concerned. The past few years have seen much progress on this front, particularly in Europe. In 2018, we found that 19 out of the then EU 28 had introduced some measures to protect whistleblowers (the highest ranking countries in that survey were France, Ireland, Malta and the United Kingdom), though all fell short of international standards to some extent[2].

Then in April 2019, the EU made a significant contribution to the protection of whistleblowers by passing a new Directive that turned whistleblower protection from a matter of best practice to a legal obligation. The EU Whistleblower Directive, or *Directive 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law*, outlines a basic standard of protection that will apply across all 27 member states of the European Union.

The Directive sets rules for who can be protected as a whistleblower and the kinds of issues they can make reports on. It defines how the idea of protecting whistleblowers interacts with other legal and ethical obligations. It provides some protections for relatives, colleagues and others who might be targeted for retaliation.

One of the most difficult questions a whistleblower will face is who they should make their report to. The Directive sets down rules about how internal (within the company), external (regulator or other outside agency) and public reporting channels should work, their duty of confidentiality to the whistleblower and procedures for investigation. It also establishes duties to publish these details so that potential whistleblowers can make an informed decision about who to turn to.

i. For a recent assessment of the costs of whistleblowing, see the Post Disclosure Survival Strategies report at https://whistleblowingimpact.org

The Directive also sets down legal protections - for the whistleblower, but also for the individuals or entities that are the subject of a whistleblower's reports. Finally, there are procedures for record-keeping and oversight in order to review whether the rules are working. The EU Directive isn't the last word on whistleblower protection, but it is a significant step forward. How well it works in practice is important, with significance well beyond the EU27.

About this report

The Directive does not apply automatically. EU Member States have until the end of 2021 to pass a law that brings national legislation into line with the standards laid down in the Directive[ii]. While the Directive sets a few eye-catching obligations, not least that every private company employing 50 people or more will need to set up or provide an internal reporting channel, there is much that is left up to the discretion of national legislators.

The text of the Directive is also clear that it should be regarded as a base level of protection and that member states should consider building on these in their own national laws. Civil society was very involved in the legislative process that produced this Directive - unusually so by EU standards - and we have assessed that it meets with international best practice in many, but not all, respects[iii].

This report is for those who want to assess whether current or proposed national law in their country satisfies the demands of the EU Directive. In addition, it provides some guidance on how member states can best resolve some of the more difficult issues in the Directive text and raise the bar in areas where the Directive is silent.

We hope that this report is also useful for those who might be charged with implementing the legislation themselves.

EU Whistleblowing Compliance Checker

This interactive online tool allows evaluation of a new or proposed law for national transposition:

https://tool.blueprintforfreespeech.net

The tool is designed to do three things. Firstly, it provides a basis to assess whether a law, or a legislative proposal, complies with the Directive. Second, it rates the law or draft law against international standards beyond the Directive, and shows areas for improvement. Finally, the tool puts forward a set of whistleblowing scenarios based on real examples from the ongoing COVID 19 pandemic. The intention of this section is to highlight how well legal frameworks might be expected to work in practice, particularly during a pandemic.

The online tool takes the form of a checklist. A walk-through of the checklist score is available here:

https://www.blueprintforfreespeech.net/en/compliance-checker-example

The online tool prompts the reader with a series of questions, which require yes/no answers. Save for the scenario questions, it should be possible to answer almost all these questions solely by reference to the legislative text. No special understanding of whistleblower law is assumed.

When all the questions have been answered, the tool provides a scorecard, indicating compliance with the Directive, broader international standards, and the practical scenarios. It also provides detailed feedback giving an analysis of the strengths and weaknesses of the proposal and suggestions on how to react to it.

The EU Directive will demand more comprehensive changes in some Member States than others. But all EU Member States will be obliged to bring in some legal changes in order to ensure compliance with the Directive. Our hope is that this report, and our online checklist, will help provide some consistency for whistleblowers across the EU and guidance for groups elsewhere thinking about improving standards of protection in their own countries.

ii. Progress towards transposition across the EU27 is being tracked in the EU Whistleblowing Meter: https://euwhistleblowingmeter.polimeter.org/

iii. Out of 23 international best practice standards we looked at, we found that the Directive fully satisfied 11 and partly satisfied another 8. The four remaining principles were either left out of the text entirely or left to the discretion of member states

Chapter 1 - What is covered

There is more than one way to approach protecting whistleblowers.

While the phenomenon of individuals coming forward to speak against the grain about important issues has a long history, the term "whistleblowing" first came to prominence in the US in the late 1960s and early 70s.

As a result, some of the first laws intended to protect whistleblowers emerged in the US. These first laws established regimes by sector - establishing special rules for particular groups of public employees and, later, the financial industry and others in the private sector. Today, whistleblower protection in the US remains a complex patchwork of different legislative schemes covering different areas of work. Later laws, not to mention the EU Directive itself have adopted a different, horizontal approach, which attempts to establish one set of rules for whistleblowers across the board.

The advantage of this horizontal approach is that it makes it easier for potential whistleblowers to understand what their rights and recourse are ahead of time, and to reduce the costs involved. In practice, under the US system, the rules and their applicability are somewhat opaque and it is essential for individuals thinking of blowing the whistle to contact a private lawyer or non-profit first in order to guide their way through the process.

The EU Directive ties whistleblower protection to the working of the Single Market, a criterion that encompasses everything from animal feed to package labelling to the security of computer networks. Unlike many whistleblower protection schemes, it covers both the public and private sectors. In effect, the Directive comes close to covering everything that the EU could possibly legislate on - but that still leaves a lot out.

The Directive covers reports of breaches of EU law. In some areas, such as national education and social care systems, the EU has only supporting competencies. This means that the EU does not directly legislate in these areas, which are left up to national governments. Reports of breaches in these areas are likely to concern breaches of national rather than EU law and, as such, are not explicitly covered by the Whistleblower Directive.

This is a gap that national governments should consider filling to ensure that the same rules apply to whistleblowers across the board. It is not realistic in practical terms to expect a whistleblower to judge whether their report concerns a breach of EU or national law. The Directive's overall approach is best replicated nationally with the introduction of horizontal whistleblower protection measures that also extend to areas governed by national or regional law. International law other than that originating from the EU will also not be within the scope of protections unless member states make a proactive choice to include it.

In addition to the limitations imposed by the EU's mandate, the Directive does also include some specific exemptions. One perennially sensitive area governed by national law is national security, defence and disclosures that concern classified information. Notwithstanding that disclosures in this area have been the subject of some of the most important public interest reporting of recent years, the unauthorised transmission, receipt or publication of classified material is prohibited with the sanction of the criminal law in many countries.

This situation is not changed by the Directive and this is one of the legislation's more obvious shortcomings. While some aspects of defence procurement come under the Directive's scope, national security and defence as an area is explicitly reserved to Member States.

Although the Directive does not establish new duties in this area, national security whistleblowing is not an area that should be ignored. In the wake of Chelsea Manning and Edward Snowden's disclosures, among others, national security whistleblowing has been the subject of international best practice recommendations and case law from the Council of Europe. These suggest that states should provide some routes of recourse for national security and defence whistleblowers, even if these channels differ from those provided for reporting in other areas.

National Security whistleblowing

The Directive leaves it up to member states to decide how to deal with national security and defence whistleblowing. There are a number of European and international standards in this area to draw on.

The Tshwane Principles on National Security and the Right to Information (2013)[3]

These detailed guidelines for balancing states' national security interests with their citizens' right to know were put together by a wide range of civil society stakeholders. They state that there is an overriding public interest in certain kinds of information, for instance evidence of serious human rights abuses (Principle 10), and that whistleblowers in these areas have access to a legal protection framework similar to that developed in the EU Directive (Principles 40–43).

Council of Europe Council of Ministers recommendation (CM Rec 2014/7)[4]

This Council of Europe recommendation on whistleblower protection, reflects many of the standards that would later be included in the Directive and also includes national security whistleblowing. It states that members may put in place "a special scheme or rules" for national security whistleblowers, but that there should be some kind of reporting channel available. The Council of Europe's Parliamentary Assembly has endorsed the Tshwane Principles on a number of occasions.

Bucur and Toma v Romania - 40238/02 (European Court of Human Rights)

The case involved a phone tapping programme revealed by a member of Romania's Intelligence Service at a press conference. The Court found that Romania's subsequent prosecution of Mr Bucur constituted an unreasonable interference with his freedom of expression rights considering the public interest in the information he revealed[5].

What is a breach?

The Directive seeks to protect those who report breaches of EU law in a range of areas. As important as the range of areas covered are the kinds of actions that meet the threshold for reportable behaviour. It is important to understand that a 'breach' in the Directive's terms this is drawn more widely than violations of the law.

The Directive defines a breach as an act or omission that is either unlawful or defeats the object or purpose of the law. Omissions in this sense include not enforcing regulations, whether purposefully or through negligence. Disclosures of information on potential breaches or efforts to cover them up are also considered as protected.

The breadth of this definition helps improve the predictability of the law for whistleblowers, who are not required to engage in an analysis of whether a particular act constitutes a violation of the law before reporting it. By the same logic, Member States may wish to consider whether the Directive's coverage is broad enough.

Waste and inefficiencies do not necessarily result from negligence and are an example of issues that may well form the subject matter of valuable reports that are not explicitly covered by the Directive. Other whistleblower protection frameworks differ from the EU's approach. The US Whistleblower Protection Act, which applies to federal employees, protects disclosures about mismanagement where this undermines an organisation's stated mission. This may be an area where Member States or individual organisations operating reporting channels may wish to expand on the Directive standards and accept reports dealing with a wide range of issues[iv].

The Directive does acknowledge this issue of predictability in its treatment of the whistleblower's state of mind. A whistleblower is entitled to protection if they had reasonable grounds to believe that their report was within the scope of the Directive, even if it later turns out that it did not.

One of the rationales for linking whistleblower protection to the functioning of the Single Market was the recognition that major problems often have a cross border dimension. The 2013 horse meat scandal brought the issue of complex supply chains to the fore. First detected in Ireland, the marketing of horse meat under misleading labels was later found to affect 16 EU Member States.

It may then be slightly surprising that the Directive does not contain explicit language about reports with a cross border dimension. Nevertheless, it is clear by implication that the these should be covered, at least in instances where the other country or countries involved are also EU Member States.

The Directive allows breaches to be reported to EU bodies, provides for legal aid in cross-border civil proceedings and cites Member States' ability to cooperate on the investigation of reports with cross-border implications as a specific topic for assessing whether the legislation is working.

Iv. Internal whistleblowing channels may also be used to raise other kinds of workplace grievances, such as interpersonal conflicts, which the Directive says employers may wish to channel to other procedures. (Recital 22)

Lost in translation - why words matter when you're defining a whistleblower

The term "whistleblower" has half a century's worth of usage and a generally well understood meaning in English speaking countries. Elsewhere it is a different matter. New terms, like the French "lanceur d'alerte" or the Dutch "klokkenluider" have been coined in a number of European languages in order to lose the negative connotations associated with other terms, which come closer to sense of 'informant' in English. How the word "whistleblower" is translated in other languages may also have a legal impact, something several countries are now having to contend with when transposing the Directive.

Spain is one of the countries that lacks a national whistleblower protection law at present and will have to make major changes as a result of the Directive. What terminology to use is itself a subject of debate. The closest term used in existing legislation is "denunciante", but it is far from a perfect fit with the terms of the Directive.

The term "denunciante", as defined in the Spanish Penal Code, is someone who makes a report to law enforcement, when this may not be the best option for a whistleblower due to the subject matter of their report or the context in which they are making it. The concept also forces the reporting person to be identified by name, which conflicts with the idea of allowing anonymous disclosures, something that is an option under the Directive. Moreover, a "denunciante" in Spanish law is restricted to making reports about criminal offences. As we have seen, the concept of "breaches" under the Directive is much broader than this.

Even if blowing the whistle is an act of justice and truth in defence of the public interest, whistleblowers may be perceived and defined in a negative way. In many languages, the terminology itself doesn't help. "Denunciante" carries an extremely negative connotation in Spanish, being associated with other pejorative concepts such as "chivato" or "soplón".

In contrast, the newer term "alertador" allows the concept of the whistleblower to be defined in more neutral language, and avoids the potential legal problems related to specific terminology.

These kinds of issues are currently being faced in several European countries. The Greek concept of Μάρτυρας δημοσίου συμφέροντος, translated as the "witness of public interest", may have similar implications for the transposition process. Because of this reason, civil society organizations are advocating for a more positive term such as "πρόσωπο που αναφέρει παράνομα ή παράτυπα περιστατικά".

Chapter 2 - Who is covered?

One of the more progressive aspects of the Directive is in the way it defines who is entitled to protection for making a disclosure, which will lead to more whistleblowers being recognized and supported in most EU Member States.

The Directive covers anyone who acquires information on breaches in a work-related context and therefore attempts to ensure that the range of work roles covered by national law is as wide as possible. By ensuring that the full range of contemporary employment relationships are captured by the legislation, the Directive again seeks to make sure there is certain predictability for potential whistleblowers.

This is something that many legislative schemes have not managed to achieve. Many whistleblower protection laws, for example Australia's 2013 Public Disclosure Act, restrict their scope to the public sector. Others have not kept up with changes in the composition of the workforce, as with the UK's Public Interest Disclosure Act of 1998. This uses a definition of "worker" that does not cover the majority of people who are self-employed, who in 2017 accounted for over 15% of the UK labour force.

Member States looking to transpose the Directive should ensure that the range of work roles covered by national law is as wide as possible, and that the full range of contemporary employment relationships are captured by their national legislation.

Since the Directive is linked to the functioning of the Single Market, it provides that any individual who encounters evidence of a matter in the course of their working lives should be entitled to protection. Within that constraint of a "work-related context", the personal scope of the Directive's coverage is broad: it includes employees, freelancers and contractors as well as their sub-contractors and employees, volunteers and shareholders. Also covered are former employees and others whose working relationship with the matter at issue is in the past; finally, it protects job applicants and others whose working relationship have yet to begin.

Nevertheless, it is important to recognise that the Directive falls short of protecting all citizens in all circumstances. For one thing, the Directive creates a separate category of "facilitator" for third parties who help or assist a whistleblower. This provision is discussed directly in Chapter 4, but journalists, trade unionists and NGOs might well themselves experience retaliation for releasing protected information and therefore merit protection directly.

The requirement for information to have been acquired in the context of work activities excludes another group. Individuals can find themselves in possession of information about wrongdoing outside of their working lives that they may want to report and see remedied. Those individuals could, of course, also suffer retaliation as a result, but are not protected under the Directive.

Examples of individuals who would not be covered by the Directive's language include a hospital patient or their relatives with concerns about malpractice. Someone who witnesses a wrongful arrest in a public place or feels that they themselves have been victimised by a public agency would also not be entitled to protection.

This is another gap that Member States may want to make good on, not least because there are examples to draw on. Some European countries have already adopted whistleblowing schemes that go further than the Directive and are open to the public as a whole: France's Loi Sapin II identifies any citizen who makes a disclosure in a prescribed manner as a whistleblower, and some Spanish regions, most notably the autonomous community of Valencia, have introduced legislation protecting any legal or physical person that uses a secure digital dropbox to report corruption. Reflecting this, a draft proposal on transposing the Directive in Spain presented by the civil society group X-Net includes protection for all citizens as potential whistleblowers[6].

One area of potential ambiguity is the difference between a whistleblower having found evidence of breaches in a work-related context and them having been in a working relationship with the individual or entity that is the subject of their report.

The former does not necessarily imply the latter. The Directive requires that someone making a report should have acquired that information during their work-related activities and that the information concerns an organisation they are or have been in contact with.

There is no requirement for a whistleblower to be in a direct working relationship with the subject of their report, or to have been in one in the past. In fact, the EU Directive suggests that companies make their internal channels open to this broader category of people who have been in contact with them (see Chapter 7 on the design of internal reporting channels).

Chapter 3 - Who is covered? (II)

The basic structure of whistleblower protection laws is that they offer protection to those who make reports when certain guidelines are followed. The EU Directive is no exception.

The Directive was put together with significant input from civil society. As a result, the Directive text reflects many of the lessons learned from how previous legislation has worked in practice.

This is particularly evident in this section of the legislation, which looks at several threshold criteria. What was the state of mind of the whistleblower when they made their report? To what extent can we assess what were they trying to achieve, and does this even matter? Is there a limit to the kinds of actions whistleblowers are entitled to take? How can we best avoid legal protections being abused?

This chapter looks at three key issues considered in the Directive in relation to thresholds for protection: good faith requirements, abusive or malicious reports and limits to legal immunity.

Good faith

Much of the media framing around whistleblowing focuses on individuals telling the truth despite opposition, with an emphasis on their public-spiritedness and moral intent - often with some justification. It is therefore tempting to look at motive as one of the defining traits of a whistleblower.

In practice, NGOs and other institutions working in this area tend to agree that good faith provisions can prove counterproductive in practice and make protections difficult to enforce for anyone[7]. Experience from the UK shows that good faith and other motivation-type requirements can enable employers to launch wide-ranging attacks on individuals in the courtroom, making it more difficult for whistleblowers to obtain protection in law and drawing the focus away from the substance of the report itself[8]. Motivation can also be used as a factor to reduce the amount of financial compensation available to whistleblowers, even when they do win their case, as is the situation in the UK and Ireland.

The Directive therefore attempts to define a threshold qualification that does not require assessing personal motivation. You do not need to speculate about the state of mind of a whistleblower to decide whether they held a reasonable belief that the information in their report was true. You need only ask whether, in their position, knowing what the reporting person did, would it be reasonable for any person to believe that the information was true. Similarly, the standard under the US WPA is that a whistleblower has a reasonable belief they are disclosing evidence of alleged misconduct[v].

v. One difference between the US and EU standards is that the Directive explicitly protects those who express reasonable concerns but „do not provide positive evidence" (Recital 43).

Good faith requirements are onerous for whistleblowers and their absence from the Directive is deliberate. Neither are whistleblowers required to establish their allegations to a legal standard of proof. Instead, a whistleblower is required only to have reasonable grounds to believe that the information in their report is true. If an investigation later determines that a report is not well-founded, the person who made that report does not lose their entitlement to protection.

In other words, the Directive also protects whistleblowers who make an honest mistake. Knowingly false reports or public disclosures, on the other hand, are not protected by the Directive and may be subject to legal penalties.

Malicious reports

One of the reasons why the motivation of the whistleblower can come into question is due to concerns about reporting systems being abused with vexatious or malicious reports that are designed to malign or harass others. Notwithstanding that it is possible for a valid report to be made with dubious intentions, the Directive does include provisions to deter abuse.

It is important to recognise that knowingly false reports attract no protection under the terms of the Directive. Those who make them are therefore risking disciplinary action from their employer and possible legal action. The Directive requires that there be "effective and dissuasive" penalties for abusing the system with information that a reporting person would have known was false. Penalties for knowingly false reports are discussed in Chapter 13.

Limits to immunity

Another threshold condition concerns legal immunity and the interaction of whistleblower protection measures with different pieces of legislation.

Whistleblowers can find themselves targeted with a range of legal provisions, including defamation, data protection, trade secrets, confidentiality and computer crimes laws. Some of these do not include any kind of public interest test or exemption.

The extent to which existing whistleblower protection laws ameliorate this situation varies between jurisdictions. The UK's Public Interest Disclosure Act, for instance, has always excluded from protection whistleblowers who "commit an offence" in the course of making a report. In contrast, Ireland's Protected Disclosures Act (2014) provides that making a protected disclosure can be offered as a defence "for any offence prohibiting or restricting the disclosure of information."

Computer crimes laws

Computer crimes legislation is framed in similar ways across jurisdictions, using definitions in the Cybercrimes Convention. Such laws create criminal offences for accessing a computer system without permission, interfering with data and for restricting access to a computer system. Computer crimes laws typically lack public interest exemptions or defences.

Use of computer crimes provisions, particularly those that prohibit unauthorised access, against journalists and their sources is on the increase. Football Leaks whistleblower Rui Pinto faces a large number of these charges. The cases of Julian Assange and Glenn Greenwald have attracted particular attention precisely because the use of these laws appears to restrict journalistic freedoms[9].

In addition, there is a long-standing problem whereby the reporting of computer security issues, which can be understood as a type of whistleblowing, often constitute a technical breach of the criminal law. Some countries, like The Netherlands, have tried to tackle this problem by issuing advice to prosecutors. Many argue that reform is needed[10].

Whistleblowers who are entitled to protection under the Directive rules can seek dismissal of legal proceedings on a range of grounds, including defamation, breach of copyright, data protection and disclosure of trade secrets.

When it comes to criminal liability, the situation is slightly more complicated. The exclusion of national security from the scope of the Directive (see Chapter 1) means that legal restrictions on the transmission of classified information are also not affected by the legislation as it stands. In addition, the Directive provides that there is an exemption to general immunity from prosecution if the acquisition or access of information does not constitute a "self-standing criminal offence". This clause causes some potential uncertainty. It is not uncommon for the acquisition of internal information a whistleblower relies on in their report to be characterised as theft. Preventing these kinds of vexatious legal proceedings - which were feature of the LuxLeaks case – was, in fact, one of the inspirations behind the Directive.

The Directive recitals clarify the situation somewhat, specifying "physical trespass or hacking" as instances where national criminal law should apply. Nevertheless, care should be taken here too. Hacking, a term that invokes inventiveness, creativity and exploration is often used, as it is here, as a kind of shorthand for unauthorised use of a computer system, but unauthorised access is itself a notoriously immutable and slippery concept.

The nature of workplaces in 2020 means that most whistleblowing cases involve digital information stored on a device or network. What is branded as "theft" to undermine a whistleblower's claim to protection could just as equally be framed as "unauthorised access"[vi]. Moreover, it is likely that many disclosures related to data protection or network security - both areas that are explicitly covered by the Directive - could also constitute technical breaches of computer crimes statutes. If immunity is not to be extended to these areas, then national courts should be able to consider the necessity and proportionality of such actions in relation to the report or public disclosure at issue.

To avoid legal uncertainty, Member States should make sure in transposing the Directive that the notion of "self-standing" is understood and defined as wholly unrelated to the ability to make a legitimate public interest disclosure.

Chapter 4 - Who is covered? (III)

The popular image of a whistleblower is of an individual whose actions mean they stand apart. Regarded with admiration by some and criticised by others, their decision to come forward makes them unusual, so that their character and motivation is as much of note as the information they bring to the fore.

As observers have noted, there is something self-perpetuating in this image. Many of those who come forward see themselves as professionals fulfilling the demands of their job description, first and foremost. Individuals in audit and compliance roles are examples of those who have a professional obligation to draw attention to issues they come across. Often it is the twin processes of negative reaction from colleagues and employers and - ironically - support from outsiders that puts an individual into that role of isolated conscientious objector[11].

In reality, whistleblowing is not necessarily a solo endeavour. Employees who go on to make reports may have allies in their place of work, who might provide a listening ear, support their interpretation of what is going on or even have made similar reports themselves. A potential whistleblower might well want to speak to colleagues before making their report in order to confirm information or obtain evidence. Experience in working with whistleblowers shows that colleagues at work, or close relatives at home are often an individuals' first port of call when they have concerns.

Those who go on to make reports may also share a place of work with their spouse or partner. In those kinds of situations, any retaliation a whistleblower experiences for making a report could also have an impact on the careers of those closest to them. It is easy to see how this could discourage some from making a report.

vi. As if to underline the point, this is exactly what did happen in the LuxLeaks case, where whistleblowers Antoine Deltour and Raphael Halet were charged with „informational fraud" as well as theft.

The EU Directive recognises these kinds of situations and extends protections to certain categories of third parties who are either connected to the whistleblower or involved in the whistleblowing process. Protections offered to individuals who make reports are extended to the colleagues and relatives who might also suffer negative consequences as a result.

The range of groups and individuals who become involved in whistleblowing cases can be much wider than this, taking in trades unions, journalists and the organisations they work for, professional organisations, NGOs, community associations and other groups. The Directive also makes some provision for these groups, albeit in a way that means that the transposition process in each EU member state will have a great deal of influence over what these protections look like in practice.

The Directive explicitly refers to existing rights for workers to consult representatives and trades unions. Beyond that, there is a clause granting protection to "facilitators", defined as "a natural person who assists a reporting person in the reporting process in a work-related context." Legal analyses of this part of the Directive have expressed concern that this clause restricts facilitator protections to individuals doing their jobs, as opposed to the organisation or legal person they work for or contract as[12].

If adopted as it stands, this might mean that an individual who works for an NGO is protected against legal repercussions for advising a whistleblower, but that the NGO itself is not. A journalist might be granted protections (over and above those already present in national law - see Chapter 9 on Public Reporting) but not the media organisation they work for.

Member States may also wish to consider expressly including co-workers or co-witnesses in the definition of facilitators. Given that whistleblowers often discuss concerns with trusted colleagues at work before making a disclosure and that they can face retaliation as a result, there should be an assurance that protection measures are available.

As we have seen, language is a key concern in promoting a culture of transparency and support for those who do make disclosures (for more details, see section Lost in translation in Chapter 1). Given that the term the term "facilitator" is a new one in this context, it needs to be translated carefully to avoid a pejorative imputation.

It takes a village - the role of civil society

Facilitators are an increasingly important part of the whistleblowing process. Much of the practical work of supporting and advising whistleblowers across the EU27 is done by civil society organisations, who have in turn both created much of the pressure for legislation and provided the information base to support those efforts.

One of the best examples is the French Maison des lanceurs d'alerte (MLA), a not-for-profit organization created by an alliance of different groups active in the field of transparency and civic rights. The MLA was launched following the introduction of Loi Sapin II, which provides legal protection for whistleblowers, but fails to establish comprehensive frameworks of support and advice. The MLA fills that gap. In Ireland, Transparency International fulfils a similar role by providing free legal advice to potential whistleblowers via their Transparency Legal Advice Centre (TCLA).

This dynamic is recognised in the Directive, but it will be up to national legislation to make these protections fully explicit. Consideration should be given to whether legal entities - such as media organisations, NGOs and professional organisations should be granted protection. In particular, EU Member States should consider the particular role civil society actors play in this field and make sure their status as facilitators is as unambiguous as possible.

Chapter 5 - Who does the whistleblower send their report to?

The ability of whistleblowers to make a choice about where to make a report - whether to their employer, to an external regulator or, in more limited circumstances, to the media - is a key element of the Directive.

These three different types of reporting channels should be presented as a series of options a whistleblower can choose between, rather than as a hierarchy with a set path through. An essential characteristic of any successful Directive implementation will be that whistleblowers are not obliged to make a report to their employer before any possible recourse elsewhere.

During the legislative process to approve the Directive, this kind of restriction, often called mandatory internal reporting, was a particularly contentious issue. It was only rejected after significant efforts. As a result, the Directive gives whistleblowers a free choice about whether to make a first report to an internal channel, or an external regulator. It is also possible to make a first report to the public or media, with some restrictions (see Chapter 9).

Many of the concerns about allowing whistleblowers a choice about where to make their report are misplaced. The overwhelming majority of whistleblowers - many studies find over 90%[13] - will typically make their first report to an internal channel in any case. Where the ability to have initial recourse to a regulator or other external body becomes critical is in the minority of cases where an employer is likely to disregard a report or, worse, penalise the whistleblower and destroy evidence when alerted to wrongdoing.

By concentrating all communications and relevant information about wrongdoing in the hands of those with the capability to dismiss, hide or modify it, insisting on mandatory internal reporting has the potential to lead to the obstruction of justice.[14].

A second potential issue with internal channels is that a large number of whistleblowing cases involve individuals being penalised for communicating information as part of their normal work duties. Those in compliance, audit and health and safety roles often have legal requirements to report issues they come across and job descriptions in other roles may impose similar responsibilities. Creating a specific protected channel for whistleblower disclosures should not create a different expectation for work-related speech of similar value that happens elsewhere. What advocacy organisations call duty speech should therefore be explicitly protected, as it has been for US government employees since the Whistleblower Protection Enhancement Act was passed in 2012. While the Directive's recital 62 states that duty speech is protected, this is not explicit in the main chapters of the legislation. Member States should consider clarifying this in transposition in order to avoid legal uncertainty.

The Directive allows Member States to encourage internal reporting, but not at the expense of providing full information to a whistleblower about how they might make a report elsewhere. The Directive also regulates the creation and functioning of external channels, operated by what it calls competent authorities. Member States have discretion to decide who these competent authorities are and there are a number of different models already being used across the EU27. These are discussed in more detail in Chapter 8.

While it is not mandatory, the Directive gives Member States the option of setting up a dedicated national authority for protect whistleblowers. This could be constituted as a basic external channel to receive, investigate and follow up disclosures (see Chapter 8) or as a body for the evaluation of how the legislation is working in practice (see Chapter 14), as well as a source of information for potential whistleblowers.

However these channels are constituted, a key requirement of the Directive is that information is made available on how whistleblowers can make a report and the different places they could do so. Internal channels are obliged to provide information on external routes of recourse. The competent authorities running external channels are required to make comprehensive information about whistleblowing procedures and what people making reports should be able to expect available "in a separate, easily accessible section" of a public website.

Chapter 6 - Who needs to set up an internal channel?

One of the major proactive features of the Directive is the obligation for employers to implement internal reporting channels (or, under certain circumstances, engage a third party to do so). This provision of the Directive is likely to be one of the most impactful and has the potential to significantly influence corporate culture and work ethics all across the European Union. The next two chapters look at who needs to implement an internal channel and how they should go about doing it.

Generally, the Directive stipulates that any legal entities in the private sector of 50 employees or more will have to set up internal mechanisms for receiving reports and following up on them. Special rules apply to organizations with staff between 50 and 249 employees: they may share resources and reporting setups with other organizations in order to keep internal costs to a reasonable level.

Furthermore, recognising that there may be reason to require special measures for high-risk sectors, the text of the Directive enables Member States to introduce more stringent obligations where necessary, for example for organizations in the environmental or health sectors. Where Member States wish to extend internal channel obligations in this way, they are obliged to notify the Commission with their reasons and the criteria relied on in their risk assessment. Where companies and private entities already have the legal obligation to establish internal channels under other Union or national legal regulations, the Directive does not introduce a lower standard.

Mirroring the broad scope of working relationships covered by the Directive (see Chapter 2), the legislation envisions that an organisation's internal reporting channel should also be open to a wider group than just direct employees. Employees of the legal entity should be able to make a report through an internal channel, but so should employees of its affiliates, suppliers, and any other person who acquired information in the context of his or her working activities related to the legal entity in question[vii].

Legal entities in the public sector have the responsibility to create and install internal whistleblowing mechanisms for their employees; special rules apply for public sector organizations in municipalities with less than 10 000 inhabitants, who may be exempt.

The Directive allows for third parties to manage the receipt and investigation of reports. An increase in the supply of these kind of third-party services is likely as the Directive's provisions are introduced into national law. Concerns have been expressed about the involvement of third parties on several fronts. One line of argument is that subcontracting out internal channels will mean that employers will be able to avoid engaging with whistleblowing in a meaningful way and there will be limited cultural change as a result in the industries that most need it.

A related concern is that reporting channels engaged as a commercial service could suffer from a conflict of interest and may not be able to act impartially, leading to a lack of trust from, and potential detriment to, whistleblowers.

Under the terms of the Directive, third party providers are obliged to comply with the same data protection and confidentiality standards as the equivalent channels operated directly. Consideration should be given to whether minimum standards to avoid conflicts of interest should also be set down in law.

vii. Non-profits are not specifically mentioned in the Directive but might be best considered as a subset of legal entities in the private sector.

Chapter 7 - What internal channels should look like

The Directive breaks new ground in establishing procedures for the reporting of wrongdoing within organizations and basic standards for how investigations should be conducted. The legislation also recognizes the importance of communication mechanisms that allow for follow-up with reporting persons - this strengthens public trust in whistleblowing schemes in general, which is crucial for effective application of the Directive.

It is clear from the Directive's provisions that whistleblowers should be able to make a report in a variety of ways. The Directive requires public and private legal entities with over 50 employees to create internal channels and mechanisms which "enable persons to report in writing and submit reports by post, by physical complaint box(es), or through an online platform, whether it be on an intranet or internet platform, or to report orally, by telephone hotline or other voice messaging system, or both".

Organizations are obliged to designate impartial persons or departments to receive and manage reports, and those charged with operating the channel are expected to maintain proper records and keep communications with the whistleblower open. A reporting person is entitled to have their report acknowledged within seven days and receive feedback within three months; Member States may choose to shorten the timeframe for feedback in selected cases, or generally.

Furthermore, these internal channels should allow reporting persons to communicate their concerns securely. Channels need to be set up in manners that allow for whistleblowers' as well as other reporting persons' identities to be kept confidential. Basic standards for confidentiality are in line with other EU regulations on the treatment of personal information, particularly the GDPR; internal channels need to reflect those regulations.

One of the major shortcomings of the Directive in general - one that runs contrary to international recommendations - is that internal channels are not obliged to allow reports to be made anonymously. The role of anonymous disclosure has become a prominent issue, particularly over the past decade due to the advent of secure digital dropboxes. This important issue is discussed further in Chapter 10.

Other requirements that the Directive makes optional for those operating internal channels might make a distinct different to how effective they are. While acknowledging the need for proper training of those responsible for handling reports, the EU has not outlined in detail any minimum standards for this, which is in any case only obligatory for those operating external channels.

Member States should make sure that legislation passed in transposition of the Directive establishes minimum standards for integrity officers to process whistleblower disclosures correctly and efficiently. At the same time, such laws should make sure that they can rely on an established organizational status preventing them from becoming a target themselves, and that all lawful actions conducted by integrity officers are protected actions.

In a similar way, while there is a requirement for those operating internal channels to keep records for the purpose of investigating reports, there is no obligation to maintain or publish statistics on the number of reports received and outcome of investigations. Employers may wish to consider doing so as a means of showing that their measures are working as intended.

Furthermore, the Directive foresees that information on the availability and functionality of internal reporting channels be communicated effectively, and that employees have access to information necessary to use them correctly.

For an example of how internal reporting channels have worked in practice, Member States may choose to look towards Italy. The Italian Legge 30 novembre 2017, n. 179 requires that public administrations put in place internal reporting mechanisms. There are currently more than 600 public administrations using secure digital

dropboxes in their internal reporting channels, based on open source technology, which is both easy to use and to replicate. The dropboxes facilitate anonymous disclosures and operators have gained experience in how to structure user interfaces to elicit actionable information. The Italian experience highlights the value of establishing digital mechanisms providing better security not only for the employees who might want to make a report, but also for managers involved and the information itself.

Secure digital dropboxes

The advent of the secure digital dropbox is one of the most important whistleblowing developments of the past decade. The expansion in the use of these secure digital reporting channels has gone hand in hand with the development of legal protections. Today, the GlobaLeaks project developed by the Hermes Center for Transparency and Human Rights and the Freedom of the Press Foundation's SecureDrop system are the two best known and most widely used secure dropbox systems.

While the initial adopters of dropbox systems were media organizations, an increasing number of entities in the public and private sector are choosing to install whistleblowing mechanisms based on secure, encrypted, open source, anonymizing technology. This technology offers several advantages, not least the ability for two-way communication between the reporting person and the managing end of the system as well as the storage of documents.

Digital dropboxes has been adapted and developed to meet different organizations' requirements, from media organizations such as Il Sole 24 ore in Italy or Mexicoleaks in Mexico, to the International Criminal Court and the Antifraud Office of Barcelona Municipality in Spain. Major companies such as Edison or GruppoFalk are also using secure digital whistleblowing mechanisms.

When secure dropboxes are properly communicated and published, they seem to be the preferred channel to report. In a 2019 report[15], the Anti-Fraud Agency of Valencia states that an overwhelming 76% of the reports were communicated by their secure digital dropbox, only 15% though General Registry and 10% though emails. At the same time, 51% of the 168 reports in 2019 where done anonymously.

Chapter 8 - What external channels should look like

Besides establishing a requirement to introduce internal whistleblowing channels, the Directive also obliges Member States to set up mechanisms that enable whistleblowers to raise their concerns directly with regulators or competent authorities.

The Directive grants Member States significant leeway in deciding what constitutes a competent authority. Member States may designate any national authority as competent, provided that it is equipped to comply with the Directive's provisions on receiving, following up and giving feedback to whistleblowers. EU countries have already adopted different structures for their external channels, and these are discussed in more detail below. Notwithstanding the wide discretion in this area, EU regulators have specifically included "relevant institutions, bodies, offices or agencies of the Union" as eligible recipients for external reports. Given that recourse to EU institutions, including European bodies such as the Commission and the EU Antifraud Office (OLAF) is defined as external reporting in the Directive, there may be merit in creating a similar situation for domestic institutions when the Directive is transposed into national law.

Whistleblowers are free to choose whether they make their disclosure internally or externally, and Member States are required to guarantee that whistleblowers have access to equal protective and support measures in both procedures. This means there are similarities regarding the requirements for internal and external reporting channels, particularly when it comes to data security, handling of reports, and communication with reporting persons. Both internal and external channels need to ensure confidentiality of a reporting person's identity, and staff members have similar duties to provide whistleblowers with feedback on ongoing investigations.

Furthermore, competent authorities operating external channels need to provide information online about reporting routes, procedures, rights and protection thresholds. Staff receiving, and handling reports must receive special training, and channels have to be designed in a user-friendly, secure manner that allows the durable storage of information. At the same time, transposition laws should take into account the particular role of whistleblowing officers and investigators by including anti-retaliation rights and well-defined roles and responsibilities.

Additional rules that apply to external reporting mechanisms only concern record-keeping and monitoring measures. Competent authorities are required to review their reporting mechanisms every three years, and to adapt them accordingly if necessary. Member States are required to report to the European Commission on a regular basis (see Chapter 14).

Reflecting that external channels could receive a significant volume of reports, the Directive includes special provisions for dealing with repetitive or trivial reports as well as triage procedures to deal with the most serious reports first. National regulations based on Directive provisions should be designed in a way that prevents abuse of these exemptions. Clear definitions on what breaches may be considered minor and thus be ignored by authorities, regulation on what happens when an investigation is delayed, as well as rules for prioritizing reports when the volume received is high are all important in this context.

Additional scrutiny must be paid to rules regarding the setup of reporting channels and procedures in order to ensure that confidentiality is respected at all times, and penalties for violation and neglect are credible and dissuasive. Sound provisions in these areas significantly strengthen public trust into protection measures offered, which is important to assure the Directive's overall objective.

Defining competent authorities

The requirements of the Directive allow Member States some flexibility in deciding how the provision of external channels should be structured. One option would be to assign different national agencies with responsibilities to

receive and handle reports in their respective areas. Following the UK and Irish examples, this could include the appointment of "prescribed persons" among existing regulatory offices. Whistleblowers could turn to specially trained staff members within agencies most suitable for dealing with their concern.

Prescribed persons systems often designate many organizations that can receive whistleblower reports and it can be unclear which specialist authority is the appropriate one in any given case. The UK and Irish experiences have shown that the ability to respond to reports effectively can vary greatly between regulators.

Other existing whistleblower protection schemes use a more centralized approach: In the Netherlands, whistleblowers can turn to the Dutch Whistleblowers Authority (Huis voor Klokkenluiders). This designated public authority was founded in 2016 not only for purposes of publicizing information regarding whistleblower rights and procedures, but also to receive and investigate reports in coordination with other relevant authorities. It also has a general oversight role encouraging best practice in other organizations.

Initial assessments of the Authority's performance in the first few years of its existence have generally found that its aims were overambitious, particularly in regard of its investigative role.

Alternatively, Member States may decide to merge provisions on external whistleblowing with existing public structures, such as anti-corruption or anti-discrimination authorities, which may already have in place certain mechanisms to represent citizen's rights. France has designated the office of the défenseur des droits, an independent constitutional authority defending individual rights and freedoms in different areas, as one of the public institutions that whistleblowers may make their reports to. This approach significantly lowers the threshold for potential whistleblowers seeking advice.

In Italy, the national Anticorruption Agency ANAC constitutes one of the public authorities whistleblowers may turn to directly, but this is only one of its functions. The institution also provides guidance and support to ethics officers responsible for receiving reports in other institutions, which helps to ensure a certain consistency in practices across organizations. The Italian agency's operations are mostly financed through revenues coming from fees private entities pay every time when applying for a public tender.

Further information on the practicalities of institutionalized whistleblower protection can be obtained from the newly formed Network of European Integrity and Whistleblowing Authorities (NEIWA). Established in 2019, NEIWA has the aim of exchanging practical knowledge on the institutionalized protection of whistleblowing and integrity promotion.

At this stage, the network counts 15 contributing organizations from 13 different European countries, among them the Italian Anti-corruption Agency (ANAC), the Dutch Whistleblowing Authority and the French Défenseur des Droits. To determine its mission, members of NEIWA signed the Paris Declaration[16] in December 2019.

The independent whistleblowing authority: How it works

International best practice strongly favors that whistleblower protection measures are accompanied by the establishment of a dedicated authority. The Directive suggests that such an institution could function as an initial port of call for whistleblowers and information center. One option is also to make it the primary recipient of whistleblower reports and to give it the role of performing initial investigations and referring these on to other authorities if necessary.

The "everything under one roof"-approach ensures that all whistleblowers have access to the same public information and can rely on equal procedures and expertise in consultation. It also provides increased legal certainty, as whistleblowers are relieved of the burden to assess which authority would be the competent one for their concern. Furthermore, a centralized approach significantly facilitates monitoring and evaluation of measures in place, and ensures equal treatment through consistency in procedures, training of staff and knowledge management.

The Netherlands became the first country in the EU to introduce a national Whistleblowing Authority in 2016[17], within three months of passing enabling legislation. The institution's tasks are threefold: to promote preventive measures in government institutions and companies, by supporting them with the introduction of sound whistleblower protection and integrity measures; to advise and consult potential whistleblowers and take in their reports; and to launch investigations into both wrongdoing and retaliation, with a focus on the latter. Formal powers include a variety of measures to allow access to relevant documentation and buildings related to investigations, as well as to hear persons involved under oath.

In 2018, operations of the Dutch Whistleblowers Authority ran on a budget of €3m, employing a staff of 15 public servants that dealt with a total of 365 requests for advice. Less than 10% of these cases referred to actual wrongdoing, and between its establishment in June 2016 and December 2018, the authority had launched a total of 19 investigations[18]. It reports to parliament on an annual basis.

Three years into implementation, experience has shown that it pays to take time in setting up such an institution. According to the Authority's own assessment, the rapid launch of the institution in a period of three months resulted in some challenges, as structures and procedures suffered from a lack in clarity. The Authority thus recommends taking enough time for setting up oversight over whistleblowing procedures and to take a holistic, comprehensive approach. Furthermore, it is important to provide adequate funding as well as training.

Chapter 9 - Disclosures to the Public

For many, whistleblowing is synonymous with journalism. It is certainly the case that, without confidential sources, much journalism, not to mention investigative journalism, would be impossible. Not only does the Council of Europe recognise that whistleblowers have their own freedom of expression rights, their contribution is necessary for journalists fulfil their 'watchdog role' in democratic societies.

Much of the visibility of whistleblowing as an issue today has been due to whistleblowers acting as sources for journalists. The acknowledgement of the significance of whistleblowing to the public interest has been enormously valuable, even if the major Panama Papers-type disclosures represent only a small subset of whistleblowing cases.

The importance of the journalist-source relationship may also obscure the kinds of public disclosures that are not mediated by journalists. In the age of social media, direct public reporting is becoming more common.

What constitutes a public disclosure for the purposes of the Directive is not defined. While much discussion of public reporting focuses on the relationship between whistleblowers and journalists, there is nothing that says that journalists necessarily have to be involved in such disclosures.

Direct publication, for instance the publication of an op-ed, a blog or a post on social media, should also be understood as types of public reporting.

Direct public reporting

The COVID 19 pandemic has brought direct reporting on social media into sharp focus. Whistleblowers in the health sector across many countries have faced disciplinary actions and other sanction for speaking out about shortages and dangers in their workplaces[19].

Existing whistleblower protection law has not always proven adequate to the task of protecting individuals in this position, as voicing concerns and observations on social media is usually not considered a protected public disclosure. Post-coronavirus legislation should give this area careful consideration, and make sure concerned practitioners do not suffer reprisals for voicing concerns about immediate threats to public health and safety.

The Directive provides considerable leeway in establishing balanced provisions. Inadequate transposition is likely to have a chilling effect on potential whistleblowers."

Source protection in the digital age

The importance of whistleblowers to the journalistic process is belied by their traditional lack of protection within that process. Traditionally, whistleblowers have been obliged to rely on journalists' ability to protect their sources, with little security should that fall through.

In some jurisdictions, journalists are granted protections under law against revealing their sources. However, source protection is a practical as well as a legal issue. That is ever more the case in an age where electronic communications and surveillance powers make discussions between journalists and their sources ever more vulnerable to tracing.

While government surveillance has deservedly received enormous attention, increased monitoring in the workplace gives rise to similar issues. Journalists need to be able to understand these risks and help their sources make their own assessments[viii]. But in this more risky environment, whistleblower protections have an important part to play.

Protections for public reporting

Whistleblower protection frameworks like the EU Directive anticipate that the majority of cases will not go public in the first instance, but do provide for the possibility of public reporting, albeit on a more restricted basis than going to an employer or regulator.

It should be said that the terms of the Directive are not particularly permissive where public reporting is concerned. A report must either "constitute an imminent or manifest danger to the public interest" with the risk of emergency or serious damage, or the whistleblower has reason to believe that using other channels will be fruitless or risky. The EU considers whistleblowing primarily as related to working conditions; in other national contexts such as the US, the act of blowing the whistle is tied much more directly to essential rights of freedom of expression.

Public reporting is also protected in situations where other reporting channels have been tried and no appropriate action has been taken in the given timeframe. The Directive recitals clarify that this covers situations where investigations have been conducted but appropriate remedial action has not been taken. If a report has been wrongly assessed as being of minor importance and an investigation closed on that basis, the recitals suggest this may be a reason to go public.

Where national laws already offer greater protections - for instance in Sweden, where source protection is guaranteed at a constitutional level - these are not affected by the Directive.

Terms like "imminent or manifest danger" set the bar for public reporting relatively high and the European Federation of Journalists has criticised these clauses of the Directive as "burdensome and labyrinthine"[20]. As with other aspects of the Directive, Member States are at liberty to introduce more permissive rules. There may be merit in revisiting the Directive's public reporting threshold in light of the practical issues raised by the COVID 19 pandemic.

viii. For more on how journalists should be working with whistleblowers in the digital age, see Blueprint's Perugia Principles (2019).

Chapter 10 - Confidentiality and anonymity

Confidentiality and anonymity are key features of sound whistleblower protection. They are distinct and different concepts. Confidentiality requirements anticipate a situation where the identity of a whistleblower is known to specific individuals who have a duty to not allow it to be known more widely.

The Directive makes the restriction of information that directly or indirectly identifies a whistleblower to authorised persons a key test of whether a reporting channel is effective.

Anonymity is different. If a whistleblower's identity is anonymous, it is not known at all. This offers the reporting person protection from any failure of the duty of confidentiality and means that they are not required to put as much trust in the system.

Anonymous reporting and secure online dropboxes

Technology has been a game changer in anonymous whistleblowing. The advent of the anonymous online dropbox, which uses encryption and other privacy enhancing technologies to obscure the identity of the person making the disclosure, has resulted in a series of high-profile media revelations. Today, anonymous dropboxes are being employed by regulators and government as well as journalistic organisations.

Unlike other anonymous methods, dropboxes allow for continuing communication with a whistleblower, which is required by the Directive. Where there are concerns about safety or lack of faith in procedure, anonymity is a good way of encouraging people to come forward with reports.

It is important to recognise that dropbox systems offer different degrees of security with particular situations in mind. The two best-known secure dropbox systems, SecureDrop and GlobaLeaks are tailored to different situations. SecureDrop focuses on those with the highest security needs and GlobaLeaks has a more flexible implementation for different types of users[ix]. Other systems are available which do not make their source code open to public audit.

Notwithstanding the prominence of anonymous disclosures in public debates around whistleblowing, the provision of anonymous reporting channels was a contentious issue during Directive negotiations. Typical concerns about anonymous reports centre on there being lower barriers to entry, which some associate with lower quality or even malicious reports. This tends not to be borne out in practice.

A 2019 survey of companies in Germany, Switzerland, the UK and France found that, where anonymous reports were accepted, around 58% were made this way. Nevertheless, in around a third of these cases, the reporting persons did not remain anonymous but voluntarily revealed their identity over the course of an investigation. In all cases, the rate of malicious reporting remained low, at between 3% and 12%.[21]

The Directive contains one firm commitment on anonymity, to ensure that whistleblowers who make anonymous reports are not deprived of protections. Where the identity of someone who has made an anonymous report becomes known, they are entitled to the same duty of confidentiality and protections against

ix. The formal threat models for SecureDrop and GlobaLeaks are available at: https://docs.securedrop.org/en/latest/threat_model/threat_model.html and https://docs.globaleaks.org/en/latest/security/ThreatModel.html

retaliation as whistleblowers who have used other channels.

Beyond this commitment, the Directive suggests that Member States consider whether to require internal or external channels to facilitate and investigate anonymous reports when received. Such a duty already exists in Italy and Australia. In addition, 75% of Dutch companies surveyed by Transparency International in 2019 said that employees could make internal reports on an anonymous basis[22].

International best practice recommends to always provide the option of anonymous reporting, in order to strengthen whistleblowers and public trust. Member States should avoid introducing whistleblowing regimes that allow for anonymous reports to be ignored, as this may lead to scenarios in which important information on peculiarly dangerous breaches ultimately remain unaddressed.

The Duty of Confidentiality

The duty of confidentiality is a key part of the Directive, which establishes rules for how this should work and a very limited number of exceptions.

Experience shows that reporting channels that fail in this duty of confidentiality do more harm than good and often make whistleblowers even more vulnerable to retaliation than they might be otherwise.

There are many examples of external channels failing in this regard. An inability to guarantee confidentiality can be symptomatic of a wider problem of regulators being too close to the industries they are intended to oversee and insufficiently independent.

The Directive lays down detailed rules about the treatment of personal data and the need for this to be restricted to authorised persons. Those operating reporting channels have a responsibility to comply with EU data protection rules, with the purpose of information collection in this context to be to ensure that an investigation can be properly carried out.

Confidentiality applies not only to personal data, but also to other information from which the identity of the reporting person could be deduced. This is a broader category than the US concept of Personal Identifying Information, which is essentially limited to that information that directly identifies an individual, such as their social security number or bank details. The Directive's confidentiality provisions extend to others involved, such as persons implicated by a whistleblower as well facilitators and supporters.

The Directive also stipulates that there should be penalties for those who breach this duty of confidentiality. These should be "effective, proportionate and dissuasive" but, as with the rest of the Directive's penalty clauses it is left up to member states to determine exactly what they should entail. Different approaches already exist within the EU. Ireland's Public Disclosure Act gives rise to a cause of action for whistleblowers if they suffer detriment due to their identity being revealed. France's Sapin II makes breaching confidentiality a criminal offence punishable by a fine or up to two years' imprisonment.

There are limited exemptions from the general duty of confidentiality, for the purpose of investigating a report or for judicial proceedings relating to a report. A whistleblower's identity may be disclosed if they give explicit consent or if it is assessed to be "necessary and proportionate" for investigation purposes, in the context of national law. Where this is the case, a whistleblower should be sent notification and an explanation in writing. While it is not explicitly provided for in the Directive, member states may wish to consider giving whistleblowers the ability to challenge these decisions, with sufficient notice to enable them to do so.

The operation of these exemptions depends to a great extent on national legal frameworks and the rights of any person or entity who is the subject of a whistleblower's report, for example the right to see their own file. Member states should refer to relevant legal obligations when putting these provisions into national law.

Chapter 11 - Legal protections for whistleblowers

As in any whistleblower protection framework, the actual provisions to protect reporting persons from suffering detriment for making a disclosure constitute a cornerstone of the Directive. In general, the law stipulates that all forms of retaliation as well as attempts at retaliation are prohibited, provided that whistleblowers have made their disclosure in the prescribed manner.

Article 19 of the Directive includes an expansive list of the types of retaliation whistleblowers may suffer. It includes the most common forms of retaliatory actions reporting persons often face, such as suspension, transfer of duties or change in working conditions, harassment and discrimination, but also measures that reflect the different working relationships covered by the Directive, such as industry boycotts that make it difficult to find new employment, reputational harm and failure to renew contracts or permits. This list is non-exhaustive; Member States should ensure that informal and social varieties of reprisal are encompassed in their definition.

Notwithstanding that the Directive's list of examples is non-exhaustive, it is possible that some retaliatory measures may not recognised as such. Due to its cross-jurisdictional nature, extradition is not always understood as a variety of retaliation, despite increases in its use against both whistleblowers and journalists[23].

Other common forms of retaliation not included in the Directive concern the refusal to provide training, assignment of duties which are not in line with a candidate's qualifications, or transfer in locations that cannot be accepted. Because the list of retaliatory measures is only limited by imagination, Member States may want to consider transposing the Directive in such a way that explicitly considers any form of discrimination against whistleblowers as sanctionable.

In addition to the prohibition of retaliation, the Directive includes other provisions aimed at strengthening whistleblowers' legal position. Firstly, it includes a waiver of liability in respect of reporting or acquisition of information, which means that whistleblowers may not be prosecuted for breaching professional obligations of secrecy or similar arrangements including workplace policies when making a report in line with the Directive.

Also, rights and remedies provided for in the Directive cannot be waived or abrogated in any kind of agreement, including settlements and non-disclosure agreements. While confidentiality agreements are undoubtedly important tools in creating a trustworthy professional environment, experiences from the UK underline the importance of considering them in such ways that they do not contradict protections measures for whistleblowers[24].

Secondly, in line with international best practises, the law includes a reversed burden of proof: Detriment suffered by whistleblowers is a priori assumed to be in retaliation for a report or public disclosure made. This means that should a case involving a whistleblower end up in legal proceedings, it is for the employer to show that any action taken against a whistleblower was not as a consequence of their report. This reversed burden of proof is an important clause in the Directive, which makes a significant difference for the ability of whistleblowers to receive the protections they are entitled to in law.

Finally, both retaliation as well as neglect of certain duties towards a whistleblower are penalized. The Directive requires Member States to introduce penalties for retaliating against or obstructing a whistleblower as well as attempts to do so, breaching the confidentiality due to a whistleblower or for bringing vexatious proceedings against them. The penalties refer to actions taken by the entity that receives a report, that is implicated by a report or by any third party. The nature of these penalties is left up to the discretion of the Member States, who are expected to take an "effective, proportionate and dissuasive" approach.

The issue of penalties for employers (and others) who treat whistleblowers badly is an important one. It is not unusual to hear whistleblowers who feel they have been failed by existing systems cite the possibility of legal

repercussions for retaliation as a key credibility test. There are examples of criminal penalties for breaking rules around whistleblower protection. Australia's PIDA makes reprisal against a whistleblower a criminal offence carrying a maximum two years' imprisonment. France's Sapin II creates a similar penalty for failing to keep a whistleblower's identity confidential. A system of exemplary or punitive damages could also form part of a "dissuasive" system of penalties.

Given that a key aim of the Directive is not only to protect whistleblowers but to ensure that their reports are properly investigated, there may be an argument for introducing penalties for failures that are not specifically cited in the Directive. A proposal for reform of the UK's aging PIDA includes a civil penalty fine regime for where the operator of an internal or external reporting channel fails to investigate or meet set standards for the treatment of protected disclosures[25].

Penalization schemes are already an effective element of many existing whistleblower protection schemes. The Irish PDA allows whistleblowers suffering retaliation to start a tort action for experiencing detriment, requesting disciplinary sanction on those executing retaliation. The first claim for penalization under the act was granted to a woman reporting health and safety issues in a nursing home. After judging her complaint, the Labor Court confirmed that she has suffered a period of suspension related to her disclosure, awarding her compensation of €17.500[26].

Penalties may not only apply to instances of retaliation, but also in cases where privacy rights are violated. The Korean Act on Public Interest Whistleblower Protection makes the undue disclosure of sensitive information related to a report, such as it's content or the identity of a reporting person, punishable by 2 years' imprisonment or a fine of about USD 18,000. Retaliation or discrimination against a public interest whistleblower may be punished with up to 1 year imprisonment[27].

Chapter 12 - Support and interim relief

Beyond providing for an extensive list of retaliatory actions whistleblowers are to be protected from, the Directive obligates Member States to introduce measures of support and interim relief. At a minimum, these have to include free and easy access to information on rights and procedures, as well as effective assistance and legal support if necessary. Furthermore, Member States may explicitly consider providing for psychological and financial support. The Directive stays silent on the question of rewarding whistleblowers financially for their actions in the context of a coordinated bounty system.

The recital acknowledges the high potential of discouragement for whistleblowers when procedures are unclear, or livelihoods under threat and stretches the importance to create an environment for whistleblowers that is as unambiguous as possible. It also suggests the establishment of an independent government body overseeing whistleblowing procedures and functioning as a public information and support center. Generally, support mechanisms should reflect the wide range of situations whistleblowers may find themselves in when in need of interim relief, and compensation mechanisms should be "real and effective" to not discourage future whistleblowers.

Existing whistleblowing frameworks provide for a variety of different measures to support whistleblowers before, during and after making a disclosure. Free legal advice and support is among the most common measures available to whistleblowers in many European countries, such as Ireland, France, Italy, Spain and others, and it is a vital one: research underlines the significant legal costs for whistleblowers going to court, even in countries where whistleblower protection schemes have existed for years[28]. Member States may wish to consider whether the compulsory legal aid requirement in the Directive is comprehensive enough to cover all the types of legal

action a whistleblower might be subjected to. In particular, consideration should be given to the costs a whistleblower might encounter during employment and other civil proceedings.

Furthermore, blowing the whistle often comes at a significant psychological cost: Many whistleblowers experience negative responses from coworkers or superiors, which may put strains on family ties or mental health in general[29]. Studies also suggest that negative experiences in these contexts may also prevent future whistleblowers from coming forward, which would ultimately defeat the purpose of the Directive. International best practice thus recommends including measures of psychological support in any solid whistleblower protection scheme[30], for example in the form of dedicated contact points. Ideally, these are accessible to whistleblowers at all stages of making a disclosure.

Member States may also consider introducing mechanisms to support whistleblowers financially if necessary. Financial support may come in different forms. In the US, bounty systems create incentives for whistleblowers to come forward by rewarding them with a share of assets saved or recovered as a result of their actions. While this approach may facilitate promoting a culture of disclosing wrongdoing, critics argue that the prospect of financial gains sits awkwardly with the public interest element of blowing the whistle.

Alternatively, financial support schemes could be designed in a manner to compensate purely for actual financial losses whistleblowers suffer as a result of making a disclosure. Different civil society organizations across Europe, such as Transparency International Germany, advocate for the introduction of a "whistleblower relief fund", designed as emergency financial support. Similarly to established bounty systems, financial means to provide for such a relief fund could be drawn from assets recovered through whistleblower disclosures. In Ireland, whistleblowers who have been unfairly dismissed as a result of making a protected disclosure are eligible to compensation of up to 5 years' pay.

Considering international best practices, EU Member States are advised to link support measures to external oversight bodies, as such an approach will facilitate the situation for whistleblowers immensely. If Member States choose to introduce a dedicated independent whistleblowing oversight authority (see chapter 8), the provision and management of support measures should be one of its key mandates.

In Bosnia, the introduction of a "whistleblower status" has proven to be an effective interim remedial measure. Under the Law on whistleblowing in the institutions of Bosnia-Herzegovina, public sector employees who report wrongdoing within their institution may not be sanctioned until investigations into their claims have been concluded; retaliation against such persons is considered an offense and is punishable by fine[31]. This mechanism has led to quick investigations into whistleblowers' reports and even reinstatement of whistleblowers.

Member States may thus consider the introduction of a certification scheme whereby a whistleblower can demonstrate the status of a pending investigation. This would substantially increase legal certainty in case of retaliation while investigations are ongoing, and facilitate the process of being recognized as whistleblower should they experience retaliation regardless. Employees whose reports are later found to be unsubstantial or even malicious, and who consciously abuse the whistleblower certification scheme should be sanctioned according to national employment law."

Chapter 13 - The other side: protections for persons concerned

The EU Directive breaks new ground in establishing a duty on those who receive reports, not just to refrain from retaliating against the whistleblower, but also to investigate the content of those reports. We have already looked at what those obligations look like, both for employers in the public and private sector and for the regulators and other organisations designated to receive second tier or "external" reports.

The duty to investigate reports brings in reciprocal obligations to the individuals or entities who are the subject of those reports. There is a need to make sure that they too are treated fairly and that their rights are respected, including the presumption of innocence and a fair trial.

The Directive looks after the interests of those who are the subject of reports ("persons concerned") in two main ways. Firstly, it includes provisions which are designed to stop whistleblowing channels being used maliciously and deter individuals from abusing the system.

Secondly, the Directive asserts basic principles of natural justice to be observed in relation to persons who are the subject of reports. Almost by definition, these principles should already be observed in EU member states. Nevertheless, investigating whistleblowing reports raises particular issues where the rights of the reporting person and the person they are reporting on need to be carefully considered.

To turn firstly to the anti-abuse clauses of the Directive, we have seen that while the threshold requirement for protection does not require a demonstration of good faith, it does specifically exclude "knowingly false" reports from protection. Indeed, Member States are required to introduce "dissuasive" penalties for those who make such reports. Ireland, for example, has introduced penalties for wilfully made knowingly wrong statements that may include up to 12 months imprisonment.

All the evidence shows that this kind of malicious use of whistleblowing rules is extremely rare. It is important that sanctions for abusive reports are drawn sufficiently narrowly that they do not present a disincentive to those who are not trying to abuse the system. If sanctions for abuse deter legislate reporting, they undermine the entire purpose of the legislation.

It may be that appropriate sanctions are already provided for in national law. This is particularly the case for public reporting - spreading false and damaging information about an individual or legal person in public likely falls under defamation law.

The risk of abuse is not the only situation where the interests of the subject of a report need to be considered. Where a report is being investigated, the subject of that reports has a right to know what the allegations against them are, and they have a right to give their side of the story. While neither of those principles are controversial, at a practical experience suggests that investigation procedures need to be carefully designed in order to make sure these rights are observed.

In the case of Ireland, some of those charged with implementing the 2014 Protected Disclosures Act have expressed concerns that the duty to keep the identity of the reporting person confidential could conflict with the right of the person concerned access their file and the detail of the allegation raised. Codes of practice have tried to grapple with the issue[32]. As suggested in Chapter 10, similar concerns have been raised about the compatibility of anonymity with the rights of persons under investigation.

Given that the Directive does allow for exceptions to the confidentiality rule where it is required by law, this is an issue where clarity of procedure is important. Those procedures should resolve at what point in the investigative process is the person concerned should be informed and how their entitlement to give their file can be fulfilled without compromising the duty of confidentiality to the whistleblower.

Other national legal frameworks may give rise to their own, different procedural issues.

Finally, the Directive establishes certain kinds of interim relief for the person concerned while an investigation is progressing. While much of this is left to the discretion of Member States, reciprocal duties of confidentiality for the person being reported on - at least in terms of the public domain - are mentioned specifically. As such, Member States should ensure that the identity of a person concerned is not be released until an investigation is completed.

Chapter 14 - Is it working? Provisions for reporting, oversight and evaluation

The Directive requires Member States to complement whistleblowing procedures with mechanisms to monitor their effectiveness. This includes an obligation for public and private entities to keep records of every report received in accordance with the necessary confidentiality requirements outlined in both the Directive as well as other EU regulations such as the GDPR.

Rules on external reporting channels foresee that competent authorities review their whistleblowing mechanisms at least every three years and adapt their procedures according to their effectiveness. Operators of external channels are expected to keep records of the individual report, which can be inspected by the whistleblower on request, together with aggregated data on the total number of reports received, the outcome of investigations and the funds recovered as a result.

Member States are obliged to submit on an annual basis information regarding the number of reports submitted, resulting investigations and, if possible, an estimate of financial damage and assets recovered to the European Commission. These statistics will, in turn, serve as a basis to review current European legislation and will provide useful insight into the effectiveness of whistleblower protection measures. At the same time, quantifying the impact of whistleblowing measures solely in financial terms disregards other positive developments, such as crime prevention in general, or an increase in public trust.

The establishment of thorough monitoring and review mechanisms is a weakness in many whistleblowing systems. In the UK, a 2013 Call for Evidence had found that whistleblowers lacked confidence in their reports being investigated, leading to a reform of reporting duties for prescribed persons taking in whistleblower reports. According to a regulation introduced in 2017, prescribed persons have to submit reports on the number of disclosures received, investigated cases as well as information on actions taken on an annual basis. This approach takes into account that consistency in procedures as well as a demonstration of transparency are important factors in raising whistleblowers' confidence that their disclosures are being taken seriously[33].

International best practice recommendations[x], too, emphasize on the need of a transparent use and application of whistleblower legislation in order to strengthen public trust in the measures taken. This includes public reporting on the number of cases, outcomes of investigations, as well as assets recovered. Operators of internal channels may wish to consider keeping aggregated statistics and publish them on a regular basis, as there is a reputational value in doing so in addition to building confidence in the system.

The Directive does not stipulate what review processes should take place at the national level, other than that certain statistics should be recorded and that a review of external channels needs to take place at least every three years. To facilitate review of the measures established, we suggest that in addition to keeping records of investigation outcomes, operators of external channels record the reasons for not launching investigations.

x. Made by Blueprint for Free Speech, Government Accountability Project, Council of Europe, Transparency International and others

Furthermore, it may be valuable to aggregate data on the outcome of reports and any legal proceedings initiated in relation to reports. This should include any proceedings for retaliation or for making a knowingly false report.

As a result of a lack in oversight from state actors, civil society organizations all across Europe have established frameworks to review how national systems and legal provisions protect whistleblowers in practise. One example is the Maison des lanceurs d'alerte, a French civil society organization monitoring the application of the French Loi Sapin II and offering support to whistleblowers[34]. This tendency is expected to be continued; Member States may wish to consider drawing from the expertise gathered by organizations, some of which have been active for decades.

To facilitate reviewing the workings of whistleblower protection measures, Member States are advised to link monitoring and evaluation processes to the respective oversight body, ideally a centralized whistleblowing authority (see Chapter 8).

Chapter 15 - Whistleblowing in the age of COVID-19

Legal protections for whistleblowers are only valuable insomuch as they meet the challenge of real-world scenarios. COVID-19 presents an important series of test cases as whistleblowers have played a critical role in furthering understanding of the pandemic from its very beginning.

Dr Li Wenliang was one of a group of medics who were reprimanded by local Chinese authorities for sharing information about the early cluster of patients with SARS-like symptoms admitted to Wuhan hospitals in December 2019. On 30 December, Li and others posted information about early cases to private discussion groups with colleagues, which were then shared more widely at a time when there was an absence of official information about the outbreak. News about the "Wuhan SARS" was trending on social media network Weibo before being censored.

At least eight medics were summoned to local police stations in the first few days of 2020 and forced to sign documents disclaiming their statements. Others appear to have received verbal reprimands from hospital authorities for sharing "false information". Dr Li contracted COVID-19 shortly after returning to work in early January and his death less than a month later met with an enormous reaction on social media.

Shortly before Dr Li's death, China's Supreme Court rebuked local authorities for reprimanding the eight medics and commented that the distribution of information in this case might have served a useful social function[35]. This acknowledgement of a whistleblower raising information in the public interest, as opposed to assisting in the better enforcement of the law marks an important milestone in Chinese legal thinking. By mid-March 2020, Li's posthumous exoneration made headlines around the world[36].

The pandemic has led to the role of whistleblowing becoming better understood in China; international organisations and civil society been quick to assert the importance of whistleblowers to the crisis elsewhere.

The Council of Europe's toolkit for member states states that the pandemic should not be used as an excuse to silence whistleblowers[37]. Over 100 civil society organisations joined a Coalition to Make Whistleblowing Safe During COVID-19 and Beyond[38]. Nevertheless, there have been distinct problems in practice.

Medics sharing information on social media has become a recurring theme of the pandemic. Italian doctors dealing with the first major outbreak in Europe issued warnings on social media about the severity of the situation, which were translated

into other languages and widely shared in early March 2020[39]. Elsewhere, healthcare professionals and other essential workers took to facebook with alerts about shortages of personal protective equipment (PPE), which were forcing them to work in unsafe conditions.

The legal position of those making reports on social media has not always been clear, with restrictions on public reporting appearing to be too narrowly drawn to protect those in a genuinely life-threatening situation. Protect's advice to UK health workers, which recommends using different reporting channels or seeking anonymity via a journalist, gives a sense of the kind of hurdles involved[40].

In practice, there have been numerous examples of retaliation. Reports about the lack of PPE, made either on social media or through other channels, have led to the suspension or dismissal of medical personnel in India, the United States and Poland, despite the extraordinary demand for skilled staff during the pandemic[41]. In the UK, there have been media reports about threatened workplace disciplinary action and social media monitoring[42] and care workers in the private sector have been dismissed for raising concerns[43].

According to media reports, academics and medics in Bangladesh have faced workplace retaliation and arrest for reporting on the spread of the virus and shortages of PPE[44]. Doctors in Turkey have been arrested and forced to make public apologies for their social media posts.[45] There have been reports of physical assaults in Russia and Pakistan[46] and the detention of several doctors in Egypt has seen the expression of concerns about the pandemic made part of a wider crackdown on political dissent[47].

The issues have, of course, not been restricted to medics. In the US, dismissals for raising health and safety concerns have been reported in workplaces as diverse as Navy aircraft carriers to Amazon warehouses[48]. Concerns about the accuracy and availability of statistical information on the pandemic have also been a feature of whistleblowing disclosures in several countries[49].

Whistleblowing is regularly identified as the most effective way of detecting fraud and is likely to prove import as unprecedented amounts of public money are put into keeping national economies afloat. Government schemes to keep workers in employment by subsidising wages are likely to become a major focus of fraudulent claims, particularly when those schemes have been started from scratch.[50] Operators of whistleblower hotlines in the UK have said that concerns about furlough fraud represent up to a third of the calls they have received, with further reports being made directly to the tax authorities[51].

The ability to report concerns about the use of technology has also been highlighted by the pandemic. Many countries have looked to technological solutions to increase the frequency and effectiveness of contact tracing, in the hope that coronavirus infections can be quickly detected, and quarantine measures applied. Notwithstanding that the effectiveness of approaches that use location data or bluetooth proximity measurements to identify individuals who may have contracted the coronavirus has not been proven, these technologies have significant privacy implications, not least for whistleblowers.

This is even more the case when participation in a contact tracing scheme is mandatory. One such mandatory scheme is Qatar's, where not downloading the national contact tracing app is a criminal offence. Shortly after the app was released, Amnesty International found a critical weakness that meant that personal data was widely accessible[52]. It is important that these kinds of issues are brought to light and no system is likely to be immune from problems.

Finally, studies have shown that democratic, transparent government schemes have proven to be more successful in tackling the challenges of global pandemics as well as minimizing resulting deaths around the world than autocratic ones that rely on secrecy[53]. Transparent information policies tend to strengthen public trust, a vital contributor to effective enforcement of emergency strategies relying on cooperation by the general public. The global COVID-19 pandemic underlines the importance of supporting whistleblowing in establishing healthy democracies that function in the interest of all citizens. Governments across the European Union should take this into account when transposing the European Directive into national legislation.

1. Blueprint for Free Speech, Gaps in the System (2018), pp.18-19, https://www.blueprintforfreespeech.net/s//wp-content/uploads/2018/03/BLUEPRINT-Gaps-in-the-System-Whistleblowers-Laws-in-the-EU.pdf
2. Blueprint for Free Speech, Gaps in the System (2018), https://www.blueprintforfreespeech.net/s//wp-content/uploads/2018/03/BLUEPRINT-Gaps-in-the-System-Whistleblowers-Laws-in-the-EU.pdf
3. The Tshwane Principles on National Security and the Right to Information (2013), https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles
4. Council of Europe, Protection of Whistleblowers - Recommendation CM/Rec(2014)7 and explanatory memorandum (2014), https://rm.coe.int/16807096c7
5. European Court of Human Rights, Bucur and Toma vs Romania (2013), https://www.right2info.org/cases/r2i-bucur-and-toma-v.-romania
6. XNet, Proposed draft law on the protection of whistleblowers (2019), https://xnet-x.net/en/template-law-full-protection-whistleblowers/
7. International Bar Association, Whistleblower Protections: A Guide (2018), p.23, https://www.ibanet.org/LPRU/Whistleblowing.aspx
8. Blueprint for Free Speech, Protecting Whistleblowers in the UK: A New Blueprint (2016), https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea06ff8d801be771a29d32e/1587572764935/Report-Protecting-Whistleblowers-In-The-UK.pdf
9. James Goodale, The Dumbwaiter Defense (2020), https://www.cjr.org/opinion/greenwald-intercept-assange-manning-wikileaks.php ; Rainey Reitman, When Computer Crimes Are Used To Silence Journalists: Why EFF Stands Against the Prosecution of Glenn Greenwald (2020), https://www.eff.org/deeplinks/2020/01/when-computer-crimes-are-used-silence-journalists-why-eff-stands-against
10. Criminal Law Reform Now Network (CLRNN), Reforming the Computer Misuse Act 1990 (2020), http://www.clrnn.co.uk/publications-reports
11. Kate Kenny, Whistleblowing: Toward a New Theory (2019)
12. European Federation of Journalists, Implementing the new EU Whistleblower Directive: A Transposition Guide for Journalists (2020), https://europeanjournalists.org/wp-content/uploads/2020/02/Implementing-Finalpages.pdf
13. Ethics Resource Center (ERC), Inside the Mind of a Whistleblower (2012), https://www.corporatecomplianceinsights.com/wp-content/uploads/2012/05/inside-the-mind-of-a-whistleblower-NBES.pdf
14. Whistleblowing International Network (WIN), WIN Legal Brief - Mandatory Internal & External Disclosures (2018), https://whistleblowingnetwork.org/WIN/media/files/win-legal-brief-focus-on-mandatory-internal-wb-12-08-181.pdf
15. Agencia Valenciana Antifraude, Memoria 2019 (2019), p. 59, https://www.antifraucv.es/wp-content/uploads/2020/03/MEMORIA_2019_CAS.pdf
16. Network of European Integrity and Whistleblowing Authorities (NEIWA), Paris Declaration (2019), http://www.federaalombudsman.be/sites/default/files/explorer/Paris_declaration_-_NEIWA.pdf
17. Dutch Whistleblowing Authority, https://www.huisvoorklokkenluiders.nl/english
18. Dutch Whistleblowing Authority, Annual Report (2018), https://www.huisvoorklokkenluiders.nl/Publicaties/jaarverslagen/2019/03/14/annual-report-2018---dutch-whistleblowers-authority
19. Protect, Covid-19, Social Media and Whistleblowing (2020), https://protect-advice.org.uk/covid-19-social-media-and-whistleblowing/
20. European Federation of Journalists, Implementing the new EU Whistleblower Directive: A Transposition Guide for Journalists (2020), p2, https://europeanjournalists.org/wp-content/uploads/2020/02/Implementing-Finalpages.pdf
21. HTW Chur & EQS Group, Whistleblowing Report 2019 (2019), https://whistleblowingreport.eqs.com/en/home
22. Transparency International, Dutch Companies Falling Short of Compliance with New EU Whistleblower Directive (2020), https://www.transparency.org/en/blog/companies-in-the-netherlands-are-falling-short-of-compliance-with-new-eu-directive-for-whistleblower-protection
23. Blueprint for Free Speech, Blueprint Principles for Whistleblower Protection, pp.6-7, https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea0704123f49c36460b8a9a/1587572801985/Blueprint-Principles-for-Whistleblower-Protection4.pdf
24. UK Department for Business, Energy and Industrial Strategy, Confidentiality Clauses (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783011/confidentiality-clauses-consultation.pdf
25. Protect, A Bill to Strengthen Whistleblower Protection, https://s3-eu-west-1.amazonaws.com/public-concern-at-work/wp-content/uploads/images/2019/11/05160222/Protect-Whistleblowing-Bill-Nov-2019.pdf
26. Ireland Department of Public Expenditure and Reform, Statutory Review of the Protected Disclosures Act 2014 (2018), p. 23, https://assets.gov.ie/8765/7e1f2c66e7c04062a25561a848e17943.pdf
27. Greece-OECD Project: Technical Support on Anti-Corruption, Whistleblower Protection in the Private Sector: Developing the Legal Framework (2018), p.21, http://www.oecd.org/corruption/anti-bribery/OECD-Greece-Whistleblower-Protection-Legislative-Proposal-ENG.pdf
28. Blueprint for Free Speech, Protecting Whistleblowers in the UK: A New Blueprint (2016), https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea06ff8d801be771a29d32e/1587572764935/Report-Protecting-Whistleblowers-In-The-UK.pdf
29. Government Accountability Project, Whistleblower Trauma, Recovery and Renewal (2015), https://whistleblower.org/uncategorized/whistleblower-trauma-recovery-and-renewal/
30. Blueprint for Free Speech, Blueprint Principles for Whistleblower Protection, https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea0704123f49c36460b8a9a/1587572801985/Blueprint-Principles-for-Whistleblower-Protection4.pdf

31. Law on whistleblowing in the institutions of Bosnia-Herzegovina (2015), http://rai-see.org/wp-content/uploads/2015/08/LAW-ON-WHISTLEBLOWER-PROTECTION-IN-THE-INSTITUTIONS-OF-BiH-en.pdf
32. Lauren Kierans, An empirical study of the purpose of the Irish Protected Disclosures Act 2014 (2019), Chapter 5, https://eprints.mdx.ac.uk/26851/1/LKierans%20thesis%20volume%201.pdf
33. UK Department for Business, Energy & Industrial Strategy, Whistleblowing Prescribed Persons Annual Reports 2018/19, http://data.parliament.uk/DepositedPapers/Files/DEP2020-0013/PP_Annual_Reports_2018-19_-_Part_2.pdf
34. Maison des Lanceurs d'Alerte https://mlalerte.org/
35. Financial Times, Coronavirus whistleblower doctor dies in Wuhan hospital (2020), https://www.ft.com/content/a82d1cac-4909-11ea-aeb3-955839e06441
36. The Irish Times, China exonerates coronavirus whistleblower who died (2020), https://www.irishtimes.com/news/world/asia-pacific/china-exonerates-coronavirus-whistleblower-doctor-who-died-1.4207837
37. Council of Europe, Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisisA toolkit for member states (2020), https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40
38. .nternational Coalition Calls for COVID-19 Whistleblower Protection (2020), https://www.blueprintforfreespeech.net/en/news/en/international-coalition-calls-for-covid-19-whistleblower-protection
39. World Economic Forum, 'Every ventilator becomes like gold' – doctors give emotional warnings from Italy's Coronavirus outbreak (2020), https://www.weforum.org/agenda/2020/03/suddenly-the-er-is-collapsing-a-doctors-stark-warning-from-italys-coronavirus-epicentre/
40. Protect, Covid-19, Social Media and Whistleblowing (2020), https://protect-advice.org.uk/covid-19-social-media-and-whistleblowing/
41. BBC, Doctor who raised concerns over PPE shortage admitted to mental hospital (2020), https://www.bbc.com/news/world-asia-india-52719110 ; The Atlantic, Hospitals Must Let Doctors and Nurses Speak Out (2020), https://www.theatlantic.com/ideas/archive/2020/04/why-are-hospitals-censoring-doctors-and-nurses/609766/ ; Wyborcza.pl, Dyrektor szpitala zwolnił położną, bo alarmowała na Facebooku, że brakuje maseczek i sprzętu (2020), https://krakow.wyborcza.pl/krakow/7,44425,25814624,dyrektor-zwolnil-polozna-z-pracy-powod-alarmowala-ze-w-szpitalu.html
42. The Times, Coronavirus: Medics 'threatened with sack' if they speak of PPE shortages, https://www.thetimes.co.uk/article/coronavirus-medics-threatened-with-sack-if-they-speak-of-ppe-shortages-qt66gbj3v
43. The Guardian, 170 care workers call UK whistleblower helpline during Covid-19 crisis (2020), https://www.theguardian.com/society/2020/may/06/over-170-carers-call-uk-whistleblower-helpline-during-coronavirus-crisis
44. Liberation, Coronavirus : le Bangladesh censure les lanceurs d'alerte (2020), https://www.liberation.fr/planete/2020/04/02/coronavirus-le-bangladesh-censure-les-lanceurs-d-alerte_1783942
45. Ahval, Turkish doctors issue apologies for coronavirus statements (2020), https://ahvalnews.com/turkey-coronavirus/turkish-doctors-issue-apologies-coronavirus-statements
46. Amnesty International, Russia: doctor who called for protective equipment detained (2020), https://www.amnesty.org.uk/press-releases/russia-doctor-who-called-protective-equipment-detained
47. Reuters, Some medics say they are muzzled in Egypt's coronavirus response (2020), https://www.reuters.com/article/us-health-coronavirus-egypt-medics/some-medics-say-they-are-muzzled-in-egypts-coronavirus-response-idUSKBN2352JX
48. NPW, Navy Seeks 'Deeper Review' In Probe Of Pandemic-Struck Warship Captain's Firing (2020), https://www.npr.org/sections/coronavirus-live-updates/2020/04/29/847842205/navy-seeks-deeper-review-in-probe-of-pandemic-struck-warship-captain-s-firing ; Time, Amazon Vice President Quits in Protest Over Company's Alleged Firings of Coronavirus 'Whistleblowers' (2020) https://time.com/5831674/amazon-engineer-quits-coronavirus-whistleblowers/
49. Florida Today, Fired DOH official to speak out, reveals new details of alleged COVID-19 data 'manipulation' attempt (2020), https://www.floridatoday.com/story/news/2020/05/22/rebekah-jones-fired-florida-department-health-manager-make-public-announcement/5247836002/ ; Channel 4 News, Can we rely on Covid-19 death figures? (2020), https://www.channel4.com/news/can-we-rely-on-covid-19-death-figures
50. Financial Times, Furlough fraud plagues Europe's drive to save jobs from pandemic (2020), https://www.ft.com/content/164ca0f9-3101-4825-b9b8-37c6549a4d4b
51. Personnel Today, Almost 1,900 reports of furlough fraud to HMRC (2020), https://www.personneltoday.com/hr/almost-1900-reports-of-furlough-fraud-to-hmrc/
52. Amnesty International, Qatar: 'huge' security weakness in COVID-19 contact-tracing app (2020), https://www.amnesty.org.uk/press-releases/qatar-huge-security-weakness-covid-19-contact-tracing-app
53. The Economist, Democracies contain epidemics most effectively (2020), https://www.economist.com/graphic-detail/2020/06/06/democracies-contain-epidemics-most-effectively

Credits

Authors:
Naomi Colvin, Bruno Galizzi and Veronika Nad

Design:
Garreth Hanley

© 2020 Blueprint for Free Speech. All rights reserved.
We'd like it if you distribute this report to those who find it useful; please do so only in its entirety and with attribution to Blueprint for Free Speech and the authors.