blueprint for FREE SPEECH

JANUARY 2021

RESPONSE TO THE PUBLIC CONSULTATION ON THE TRANSPOSITION OF DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 23 OCTOBER 2019 ON THE PROTECTION OF PERSONS WHO REPORT INFRINGEMENTS OF UNION LAW ("WHISTLEBLOWERS").

PREPARED AND PRESENTED BY

BLUEPRINT FOR FREE SPEECH

Response to the PUBLIC CONSULTATION ON THE TRANSPOSITION OF DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 23 OCTOBER 2019 ON THE PROTECTION OF PERSONS WHO REPORT INFRINGEMENTS OF UNION LAW ("WHISTLEBLOWERS").

In response to the public consultation submitted by the General Technical Secretariat of the Spanish Ministry of Justice, on 07 January 2021, in order to obtain "the opinion of the subjects and the most representative organisations potentially affected by the future rule on the following aspects:

a) The problems that the initiative is intended to solve;
b) The need and timeliness of its approval;
c) The objectives of the regulation;
d) The possible alternative regulatory and non-regulatory solutions".[1]

With the intention of strengthening as much as possible the provisions to be taken into account in the transposition process, in order to generate an ambitious and responsible proposal, the following specific contributions to the specified consultations are provided.

ABOUT BLUEPRINT FOR FREE SPEECH

Blueprint for Free Speech is an international non-profit organisation working to defend freedom of expression and access to information. Part of this work is the protection of people who report information in the public interest. It has participated in various legislative processes, contributing to the development of legal and cultural standards of protection in member states of the European Union, Mexico, Brazil, Taiwan, Ukraine, the United Kingdom, Australia, and South Africa, among others.

Based on Blueprint's *Principles for the Protection of Whistleblowers*, which reflect international best practice in the field, we have developed numerous reports and studies on protection measures in law, as well as how they work in practice. Among them, the recently published "How to protect whistleblowers: A practical guide to transposing the European Directive."

We have also produced the first online tool to provide an in-depth assessment of laws and legislative proposals to protect whistleblowers as evaluated against the requirements of the EU Directive. The online tool further rates such draft or actual laws against other international standards and known COVID-19 whistleblower risks.

The online tool is a free-to-use, original resource that aims to strengthen national transposition processes in each of the EU member states, as well as further afield as other countries begin to look at the EU Directive as a new standard. Both tools, developed in the context of the EU-supported Expanding Anonymous Tipping (EAT) project, are used as references for this contribution.

The online tool will provide a useful way of checking any draft legislation against international standards as well as the Directive.

As an international civil society organisation, Blueprint works in Spain in collaboration with other social and civil organisations, academics and public servants to achieve a successful transposition of the Directive in Spain. We are international leaders in this field. Among our other activities in Spain, we have convened groups of experts across government, law and academia to review and advance, as well as coordinating a coalition of more than 15 not for profit organisations to jointly request the opening of this legislative process to the community. The ABRE Coalition has agreed on a number of key points for transposition.

Blueprint's submission is written by Bruno Galizzi, Naomi Colvin, Veronika Nad, and Dr Suelette Dreyfus on behalf of Blueprint for Free Speech. Language translations are by María Luz Climent Mascarell. Blueprint gratefully acknowledges legal support from Latham & Watkins.

Contact: brunogalizzi@blueprintforfreespeech.net

INTRODUCTION

Whistleblower protection is not only an anti-corruption measure; it is also an emerging human right. In particular, we see whistleblowing as a logical extension of the right to freedom of expression. **It is the right to dissent from wrongdoing.**

Speaking up in exercise of this right is what must be protected. The importance of this particular right is of great significance in Europe, given its history.

Laws that protect whistleblowers should draw attention to the human rights aspect as part of the intent of the legislation.

They should also reference the importance of freedom of the press as a principle, and that, in certain circumstances, the channel between the whistleblower and the media must be recognized as a protected one.

A free press is an important failsafe mechanism for a functioning democracy; it defends against not only corruption but also abuse of power. The modern relationship between the whistleblower and the media has become vitally important in the public interest, and thus should now be explicitly protected in any new whistleblower protection law.

Whistleblower protection needs its own stand-alone comprehensive law. In our experience as an international NGO, this is the most effective approach. While whistleblowing can overlap with anti-corruption activities - which are also important - it should not be subsumed under an anti-corruption law. They should be two separate and distinct pieces of legislation, working in legal harmony. Whistleblower protection also involves other areas than crime-fighting, including freedom of the press and the protection of the whistleblower-journalist relationship in an open democracy, as well as human rights.

Some of the proposals put forward in this submission propose a new way of framing thinking about the law and whistleblowers. Yet, there is increasingly a public mood internationally for this.

We have been conducting a national research project in Spain. Results from our forthcoming report indicate that there is strong support among Spaniards for supporting, not punishing, whistleblowers - even if they reveal information from inside an organization.

INTRODUCTION

A national survey, conducted for us by IPSOS, based on a representative sample of 2,174 interviews, revealed:

- 71% of Spaniards surveyed believe whistleblowers should be supported even if they reveal information from inside an organisation.
- Just 16% disagree and believe whistleblowers should be punished instead.
- One striking thing about the data collected was the strong support for protecting whistleblowers across different groups in society. Categories of the surveyed population analysed by gender, age, education levels and marital status all showed a firm majority of support, ranging from 64% in the lowest group rising to 77% in the highest.
- People with more academic training (74%) are more in favour of doing something about it. However, 66% of those with basic education are also in favour of taking action in the event of irregularities.
- In terms of age, those who feel most responsible for taking action are between 35 and 54 years of age. Nearly three out of four (73%) feel it is appropriate to alert even if they have to reveal secret information.
- Analysis of support by region showed the highest support for protecting whistleblowers in the regions of Cantabria (86%) followed by Murcia (77%).
- In the biggest regions of Spain: Madrid and Cantaluña the support is 72%.
- Married (71%) and Single (73%) people across Spain had similarly high levels of support, with Divorced, Widowed and Separated people (64%) also revealing the desire to protect whistleblowers at a lower rate but still majority.

Whistleblowers do not receive protection under Spanish law currently. Spain does not just lag behind the Directive, it is well behind most other European countries in this since many already have some or many protections in place.

The requirement for national transposition of the Directive creates not just a requirement for Spain; it creates an opportunity. The opportunity is **for Spain to lead Europe** in this area not just catch up. Reframing thinking in a law reform sense beyond simply ‘an anti-corruption tool’ is one way to do this.

ANSWERS TO SPECIFIC QUESTIONS

1. ***In relation to the power of Member States to extend protection in their national law to other areas or acts not covered by Article 1(1) of the Directive:***

    - ***Should the protection of the complainant be extended to any matter of national law beyond the rules originating in European law?***

Preamble: words matter

The term *whistleblower* has been in use for more than 40 years and is generally well understood in English-speaking countries. Elsewhere, however, it is different. Newer terms such as *lanceur d'alerte* in French or *klokkenluider* in Dutch have been coined in a number of European countries to shed the negative connotations associated with other words and are closer to the meaning of "*informant*" in English. How the word "*informant*" is translated in other languages can also have a legal impact. This is something that a number of countries are having to deal 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 significant changes as a result of the Directive. The terminology to be used is itself a matter of debate. The term most commonly used in existing legislation is "*denunciante*", but it is far from being perfectly in line 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 route may not be the best option for a whistleblower due to the subject matter of the report or the context in which the report is made. The concept also requires the person to be identified by name, which conflicts with the idea of allowing anonymous alerts, an option that the Directive does provide for. Moreover, the "*whistleblower*" in Spanish law reports criminal offences. The concept of "offences" in the Directive is much broader.

Additionally, the term "denunciante" has a negative connotation in Spain, associated with other concepts such as "snitch" or "informer", which would limit the scope that such legislation could bring to Spain, fostering a cultural and social transformation towards a revaluation of citizen participation.

Therefore, we propose to adopt the term "*alertador*" or "alerting person", thus establishing a difference between the definitions established in Spanish law and in line with the Directive.

As a reference, we propose the following definition.

> *Alerting Person: any natural or legal person who, having a reasonable conviction as to the veracity of the information to be transmitted, brings to the public's attention possible irregularities, infringements, actions or omissions that produce illicit or bad practices that are contrary or detrimental to the general interest or contrary to the legal system or duly established ethical codes, and which have occurred, are occurring or are likely to occur in the sphere of public administrations or the public sector and in private companies or entities. The reporting person shall bring this information to the attention of competent authorities or third parties by means of personalised or anonymous communication or disclosure through a specially established alert channel or by public dissemination. The motivation of the alerting person shall be irrelevant, reasonable belief in the veracity of the information at the time of submitting the alert being sufficient.*

Material scope

Article 2(1)(a) to (c) of Directive 2019/1937 stipulates the areas, in which breaches of Union law are designated to be reportable. Due to the limited nature of its legal mandate, the European Union only has the legal competence to issue legislation in selected areas. Therefore, the Directive on the protection of whistleblowers is limited to those issues relating to Union law, and accordingly only sets out to lay down "common minimum standards" (Article 2(1)).

However, in order to guarantee a more comprehensive protection and ensure equal treatment and legal certainty for all whistleblowers, we propose to expand the material scope of the transposition law to include:

(i) breaches of national laws, international laws (that are not Union law), and other regulations and codes that protect public interests;

(ii) breaches in other areas than those specified by the Directive.

(iii) Moreover, we suggest to clarify that a "breach" is to be understood broadly and also includes cases of omission, abuses negligence and waste; and (iv) that both potential and actual breaches are included.

(i) Inclusion of national and international (non-EU) laws: To ensure a uniform application of the transposition law, the scope of application should be extended to include breaches of national Spanish laws and regulations, international law that is not Union law as well as any violations of other regulations and ethic codes that serve the public interest. Such an extension would decisively contribute to legal certainty for potential whistleblowers, since even for legally qualified whistleblowers it would regularly not be apparent whether the infringement concerned Union, other international or national law. This uncertainty – and the risk of not being protected in case of a reporting of the "wrong" infringement – may discourage whistleblowers from making reports.

(ii) Inclusion of other than the stipulated areas: Together with an inclusion of national laws and regulations, we propose to expand the areas to which the transposition law applies.

The Directive requires regulation on matters of Union competence. This means that some areas, such as **the national education system and the health system**, are left to national governments. An inclusion of these fields into the protective scope of the transposition law would be crucial due to the tremendous importance of such areas for the public and high risk associated with breaches in these fields.

In addition to the limitations imposed by the EU mandate, the Directive also specifies some areas that are exempted from coverage.

One area that is always particularly sensitive and governed by national law is the area of national security, defence and disclosure of classified information. Although disclosures in this area have been the subject of some of the most important public interest disclosures in recent years, the unauthorised transmission, receipt or publication of classified material is prohibited and criminalised in many countries.

Spanish law should allow for genuine whistleblowing in the national security and related sectors, which under EU law remain under national control. Irregularities occur in all sectors, and whistleblowers in the national security and related services deserve the same legal protection as whistleblowers in other parts of society.

Recognising that disclosure of information in these sectors is a particularly sensitive issue, the draft provisions should be guided by the Global Principles on National Security and the Right to Information (Tshwane Principles). This ensures a balanced representation of both national interests and the rights of whistleblowers.

As per the Council of Europe‘s Council of Ministers recommendation CM rec 2014/7, employees in national security, defence and other sensitive roles should have recourse to a whistleblowing channel. These procedures can be different ("a special scheme or rules“) from those provided for workers in other sectors.

Other areas that we suggest to be included are:

(l) subsidies or promotional activity
(m) Public service
(n) town planning
(o) infringements affecting foreign financial interests in international transactions.

(iii) Broad interpretation of the term “breach”: We propose that the transposition law clarifies that a “breach” is to be understood broadly and also includes cases of omission, negligence and waste. The Directive defines an infringement as an unlawful act or omission. Omission in this case encompasses the failure to enforce, either on purpose or through negligence. Disclosures of information about possible infringements or efforts to cover up infringements are also considered to be protected.

Waste and negligence are not covered by the Directive. Their inclusion is however crucial to avoid gaps of protection. The purpose of whistleblowing (and the protection of whistleblowers) is, among others, the protection of the public from harm resulting from breaches of the law. Such harm can equally result from acts of negligence or waste.

(iv) Applicability to both potential and actual breaches: Taking into account the complex nature of infringements and related evidence, it should be clarified in the transposition law that the protection applies to the reporting of both breaches that have already occurred as well as such for which there is a concrete suspicion, supported by evidence, that they will materialize. This is in line with Article 5 No. 2 that covered by the Directive is the reporting of "information on infringements, information, including reasonable grounds for suspicion, relating to actual or potential infringements".

For reference, we propose the following definition of an alert (or whistelblowing report):

> *verbal or written information, nominal or anonymous, of possible irregularities, infringements, actions or omissions resulting in wrongdoing or malpractice that are contrary or detrimental to the general interest or contrary to the legal system or duly established codes of ethics, and which have occurred, are occurring or are likely to occur in the field of public administrations or public sector and in private companies or entities.*

- ***In which specific areas or subjects does the protection of whistleblowers need further strengthening?***

In addition to expanding the material scope of the Directive (as laid out above), it must be ensured that whistleblowers are adequately protected from retaliatory measures, civil liability and, above all, criminal prosecution.

In order to prevent whistleblowers from being deterred from making a report, the transposition law should include provisions that protect whistleblowers from criminal prosecution in cases where may have to commit minor breaches of law as a necessary part of making their disclosure.

Whistleblowers can find themselves targeted with a range of legal provisions, including defamation, data protection, trade secrets, confidentiality and computer crimes laws. 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, for example, currently faces a large number of such charges in ongoing criminal proceedings in Portugal.

But the risk of being prosecuted for computer crimes are not only an issue for 'outsider' whistleblowing in controversial cases. The nature of workplaces in 2021 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.”

This is in fact exactly what happened in the case of Antoine Deltour, whose Luxembourg

prosecution included computer crimes as well as theft charges. Care should be taken in interpreting the sense of a "self standing criminal offence" to ensure that measures that are necessary in order to make a disclosure do not attract criminal or civil sanction.

In addition, there is a long-standing problem whereby the detection and reporting of computer security issues, such as data breaches, can constitute a technical breach of the criminal law. See for example: https://www.cbc.ca/news/canada/nova-scotia/freedom-of-information-request-privacy-breach-teen-speaks-out-1.4621970.

Data protection and network security are explicitly areas that are covered by the Directive. Moreover, prompt notification of data breaches is a cornerstone of European Data Protection law. Government signals in this area should be clear, so as to not undermine these public policy goals.

Vagueness in a law means that a whistleblower can not be confident ahead of time whether or not a disclosure will be protected. We know from first-hand accounts that some whistleblowers do read the legislation to understand the risk to themselves before making a disclosure.

Whistleblowing should focus on the disclosure's validity not the person making the disclosure. A fair and proper investigation must be made, based on the facts not on the nature of person making the disclosure. There must be protections against retaliations, and these must be substantial to ensure compliance.

One possibility is to include a provision in the transposition law (or alternatively the criminal code) that whistleblowers, who commit a criminal offence for the purpose of obtaining or securing information to be disclosed, shall not act unlawfully if the whistleblower's – and the public's interest – in the disclosure of the disputed information outweighs other potentially impaired interests, e.g. those of the whistleblower's employer.

At the least, it should be clarified in the law that the fact that the whistleblower acted for the purpose of reporting unlawful conduct – and therefore contributed not only to the public's interest but also assisted in maintaining the integrity of the legal system as a whole – should be taken into consideration in criminal proceedings and potential sanctions should be reduced or removed accordingly.

2. ***In relation to the personal scope provided for in Article 4 of the Directive:***

   - ***Which public sector entities should fall within the personal scope of the Directive?***

Preamble:

The Public Consultation defines the **subjective scope** as the "identification of other subjects obliged to implement whistleblowing channels in both the public and private sphere", while the present one refers to Article 4 of the Directive, referring to the **personal scope** which defines the persons to whom the Directive applies. Emphasising the utmost need to clearly define and differentiate between the two, views on both are shared below.

Personal scope (potential whistleblowers)

The transposition of the Directive extends protection to a wide range of persons employed or otherwise affiliated with both public or private entities. This is definitely a positive point, given that there are laws that only cover the public sector or certain types of employment relationships in the private sector (e.g. excluding the self-employed).

Accordingly, protection should be granted not only to employees but to all workers in the public or private sector, in a civil service or employment context, both self-employed and employed, shareholders of legal entities, (sub-)contractors, suppliers as well as trainees, volunteers, board member, students or interns. An example of this might be construction workers that obtain knowledge on environmental violations on a construction site. At the same time, former employees or candidates for employment with public or private legal entities who access information in the process of interviewing or negotiating working conditions will be protected.

However, it is necessary to extend protection to the maximum extent possible so that any natural or legal person can enjoy protection, regardless of their employment status or link to disclose the information. This breadth of protection is one of the potentialities of the legislation to be transposed in order to maximise its effects.

One area of possible ambiguity is the difference between a whistleblower who has found evidence of wrongdoing in an employment context and one who was otherwise affiliated, e.g., who has (had) a personal relationship, with the person or institution that would be the subject of the complaint. The Directive requires that a whistleblower has acquired that information in the context of an employment relationship and that the information relates to an organisation with which he or she is in contact or has been in contact in the past.

However, we recommend protecting **all natural or legal persons** who disclose information of public interest, in line with the ideas shared in the previous sections. This is not only employees. Only a broad applicability of the transposition law will ensure that the public is adequately protected from harm caused by unlawful conduct. The source of the information and the relationship between whistleblower and concerned company should not be decisive in this regard.

It is important to note that the Directive avoids making a motivational judgement on whistleblowers, but rather establishes the need to establish a **reasonable belief in the veracity of the information shared at the time the alert is made**. According to the Tshwane Principles on National Security and the Right to Information (2013), this is a criterion that articulates objective and subjective elements in the definition of protection.

Protection of third parties

Facilitating persons, who may play a direct or indirect role before, during and after the alerting process, are included within the scope of protection. Equivalently, third parties related to the alerting person, such as **relatives** (spouses, ascendants and descendants of two levels, and other close relatives) or close affective relationships (without the need for a formal link) will be protected as well as persons belonging to their **work context**, being direct work colleagues, or persons belonging to the same legal entity.

At the same time, the importance of extending protection to l**egal entities and other assets owned by the whistleblower** is stressed, in order to prevent reprisals or dissuasive actions from being implemented in this way.

- ***Should a broad conception of the public sector be adopted, taking as a reference the subjective scope of application of Law 19/2013, of 9 December, on transparency, access to public information and good governance? Should constitutional bodies and/or political parties be included?***

Subjective scope - obliged subjects

The broadening of the subjective scope is fundamental so that not only those legal entities with the obligation to establish reporting channels are covered by the law, in particular constitutional bodies and political parties.

This is particularly important given that corruption in political parties has proven to be a significant problem in the past. In general, democratic systems benefit from the establishment of checks and balances. The best means of ensuring constitutional bodies stay independent is to put mechanisms in place to keep them accountable.

We therefore suggest to expand the Directive's scope in line with Law 19/2013 of 9 December 2013 on transparency, access to public information and good governance, to include:

a) The General State Administration, the Administrations of the Autonomous Communities and the Cities of Ceuta and Melilla and the entities that make up the Local Administration.

b) The Cortes Generales, the Ombudsman, the Court of Audit, the Council of State, the General Council of the Judiciary, the Economic and Social Council, the Council for Transparency and Good Governance, the Independent Agency for Fiscal Responsibility.

c) Public law corporations at State, Autonomous Community or local level.

d) Autonomous bodies, state agencies, trading companies dependent on public administrations, owned or effectively controlled by them, public business entities and public law entities which, with functional independence or with a special autonomy

recognised by law, are entrusted with regulatory or supervisory functions of an external nature over a specific sector or activity, independent administrative authorities and state-level public universities.

e) Associations and foundations set up by the public administrations, institutions or entities referred to in the letters listed above in this same section.

f) The activities of natural or legal persons that contract or subcontract with the aforementioned public administrations, institutions or entities, and the concessionaires and recipients of public aid or subsidies granted by the public administrations, institutions or entities listed above in this same section.

g) Political parties, trade union organisations and employers' organisations at state level.

h) The managing bodies and common services of the Social Security, as well as the mutual insurance companies for accidents at work and occupational illnesses that collaborate with the Social Security.

i) Any public bodies and public law entities linked to or dependent on the Public Administrations.

j) Any entity, regardless of its legal form, which is majority financed by the aforementioned public administrations, institutions or entities, or subject to their effective control.

k) National, regional (European) or international private legal entities.

3. ***In relation to the obligation to establish internal complaints channels and mechanisms set out in Article 8 of the Directive:***

- ***3.1 Should Spain avail itself of the anonymous reporting option?***
- ***Should anonymous reporting be recognised in both the public and private sectors?***

Anonymity is necessary to protect whistleblowers, in particular in a country like Spain, where those who disclose information about crimes and malpractice are still negatively perceived as "traitors" and face the risk of prosecution and sanctions.

Research shows that the option of anonymous reporting encourages whistleblowers to come forward where they perceive to be a risk of retaliation or where systems are untested.

High profile media reporting has often drawn on disclosures from whistleblowers who have decided to remain anonymous. Reporting on Wirecard, Dieselgate and the Panama Papers eloquently shows why anonymous disclosures should not be ignored.

Through Blueprint's recent work on the EU funded project Expanding Anonymous Tipping (EAT), we have found that public authorities who do adopt online anonymous reporting methods invariably find them extremely valuable.

Germany‘s BaFin estimates that 85% of the actionable reports they receive come through their secure anonymous dropbox. Greece‘s Public Procurement Authority – which set up a dropbox as part of the EAT Project – reports having received three actionable reports in their dropbox‘s first month of operation.

There is already extensive experience in Spain to ensure the recognition, processing, investigation and use of information received through anonymous communications in both the public and private sectors.

The 2019 Report of the Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community (AVAF), published on 30 March 2020, recognises the existence and use of anonymity as a tool for securely disclosing information, reaching 51% of communications in the last year.

This first-hand testimony is powerful but we think adoption will be faster with endorsement of the principle of anonymous disclosure at the national level. We have found that potential adopters of dropboxes have been hesitant to do so where the national legal situation is unclear.

There are other legal instruments that already establish sector-specific criteria in relation to the creation of internal channels. Article 26 bis of Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing, obliges all regulated entities to establish "internal procedures so that their employees, managers or agents can communicate, even anonymously, relevant information on possible breaches of this law, its implementing regulations or the policies and procedures implemented to comply with them, committed within the regulated entity". The regulated entities designated by the Law include both public and private legal entities, although the latter is affected to a greater extent.

Similarly, Article 24 of the aforementioned Organic Law 3/2018 of 5 December 2018 on the protection of personal data and the guarantee of digital rights, establishes that "[i]t shall be lawful to create and maintain information systems through which a private law entity may be made aware, even anonymously, of the commission within it or in the actions of third parties contracting with it, of acts or conduct that may be contrary to the general or sectoral regulations applicable to it.”

Information provided anonymously has even led to numerous recent rulings in Spain, most notably that handed down by the Criminal Chamber of the Supreme Court on 6 February 2020 (35/2020), which has allowed criminal acts in the private sector to be brought to light.

With regard to the public sector, Articles 62 and 63 of the Law on Common Administrative Procedure for Public Administrations on the initiation of proceedings by complaint, require the identification of the complainant, which will have to be amended in order to allow for anonymous alerts (or complaints). However, following the Judgment of the Supreme Court of Justice of 3 April 2018, this has not prevented the consideration of information provided anonymously.

The law transposing the European Directive should recognise and protect communications that are made anonymously, as well as those who have chosen to do so anonymously, regardless of whether the information or the person is linked to the public or private sector.

- ***Should Spain ensure that private entities with less than 50 employees establish internal whistleblowing mechanisms and/or channels?***

There are certain areas that are excluded from this limiting criterion, in particular the financial sector, which may have a high impact. We believe it is relevant to be able to extend, given the present pandemic circumstances, to the health sector, as well as to areas that may have an impact on the environment.

- ***In which specific sectors should companies in particular be required to have internal whistleblowing channels, and should Spain exempt public entities with fewer than 50 employees from the obligation to establish internal whistleblowing channels and/or mechanisms?***

In our view, Spain should not exempt public entities with fewer than 50 employees form the obligation to establish internal whistleblowing channels and/or mechanisms. Internal reporting under public law are to be set up at local authority level to ensure proximity to both the citizens involved and the facts of the alleged breach.

Moreover, small public entities with less than 50 employees may be tasked with highly specialised tasks that require a local analysis and processing of potential complaints. If resources (with regard to funding and personnel) are at issue, a compromise could be to allow for common reporting channels of several entities at the local level, e.g. of several municipalities.

If the burden is too heavy for smaller organisations, the cut off for the number of employees could be dropped down to 40 employees.

All companies and public sector organisations above a minimum size should be require to have some form of internal whistleblowing policy and channel.

Further, the Directive explicitly provides for exceptions to the limiting criterion for the creation of internal channels as defined in Annexes I.B and II (refer to Article 8, paragraph 4). The sectors covered therein are those corresponding to:

- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Transport security;
- Environmental protection.

If Spain decides to exempt entities with less than 50 employees from the obligation (which we would not recommend, see above), other areas should be added to the list of those not to be exempted from the obligation, including (but not limited to) public health, data protection, food safety, and others.

- ***Should whistleblowing channels be allowed to be managed both internally by a designated person or department and externally by a third party, notwithstanding the fact that the responsibility for the management of the channel lies with the internal body of the company or entity?***

The Directive provides for the possibility of appointing third parties to manage channels for private sector entities with between 50 and 249 employees. It requires special sensitivity to regulate the conditions and security standards that these third parties will have to respect and put in place to avoid conflicts of interest and possible breaches in the security of information, both when receiving it and when storing and handling it for investigative purposes.

4. ***In relation to the obligation to establish external reporting channels in Article 11 of the Directive:***

- ***Should provision be made for the procedure to be closed in the case of a manifestly minor infringement?***

Although the Directive provides for the possibility of closing procedures in the case of minor infringements, we believe that this criterion is extremely difficult to implement in a homogeneous way for all the areas of law. Information that constitutes an alert must be received, analysed and investigated until it is clear whether it can be considered an indication on which to act and proceed appropriately.

- ***Should provision be made for the possibility to close the procedure in respect of repeated complaints which do not contain significant new information on infringements compared to a previous complaint for which the relevant procedures have been concluded, unless there are new factual or legal circumstances which justify a different follow-up?***

It is necessary to analyse and investigate all communications received in order to identify whether or not they contain new and significant information on infringements that may have been received previously. Establishing homogenous mechanisms that enable (or encourage) the aggregation of communications or their rejection therefore seems to be risky and should only be made possible in exceptional cases under clearly defined conditions.

5. ***Should an independent administrative authority be created to receive, respond to and follow up on complaints submitted through external channels or should the functions be entrusted to an existing authority?***

The creation of a new independent, autonomous and impartial administrative authority seems to be a common consensus, underlining the full need to move forward and pay due consideration to the importance of the subject matter. A central oversight body secures equal treatment, legal certainty and coordinated procedure.

The centralisation of the "external channels" in a single existing authority seems to be unfeasible in terms of volume and capacity for processing communications in due time and form and would unduly limit a whistleblower’s potentially addressable channels.

However, the law transposing the Directive will have to extend and improve the possibilities for those who choose to report, not limit them further. For this reason, we believe that other external channels such as the National Markets and Competition Commission, the Spanish Data Protection Agency or anti-fraud agencies or equivalent authorities (e.g. Courts of Accounts) should also be competent to receive and process complaints in their specific areas of expertise. However, in order to be capable of doing so, they must establish reporting channels in accordance with or adjust existing reporting channels to the level set out in the Directive.

The independent authority should establish collaboration and coordination with other external channels legally designated to receive complaints, as well as with the Public Prosecutor's Office, the Courts and Tribunals, when required, through technical assistance and the issuing of expert reports by civil servants in its service, specialised in legal-administrative, economic, accounting and administrative control matters, and with in-depth knowledge of the administrations and their procedures.

The authority should - first and foremost - guarantee the protection of whistleblowers, without making this conditional on the granting of a whistleblower "certificate". Rather, the authority should ensure compliance with the law and may intervene to ensure effective protection.

The appointment procedures for any oversight institution should be designed in such a way as to ensure independence and accountability. We also endorse regular – at least annual – reports to the Congress with data being made public. Statistics should be reported in such a way as to ensure confidentiality and minimise the risk of re-identifying whistleblowers, for instance by adopting Differential Privacy techniques.

6. ***In relation to Article 23 of the Directive, what kind of applicable sanctions do you consider to be effective, proportionate and dissuasive?***

Among the authority's competencies, the establishment of sanctions in cases of non-compliance with the provisions of the law is one of the most important. Penalties must be graduated and defined in the law, and the competent body must be able to graduate them in accordance with the principle of proportionality, taking into consideration the degree of culpability or the existence of intent, the damage caused or the risk resulting from the infringements and their transcendence, as well as the continuity or persistence of the infringing conduct.

On the other hand, **we want to draw attention to the risks of sanctions to be imposed on persons who have made allegedly "malicious" communications.** This mechanism is and has been the most widely misused for persecution, delegitimisation and aggression against whistleblowers. The law should establish mechanisms to prevent malicious communications by focusing on the analysis of the veracity of the information through verification. The focus should be on the information, not on the alerter. Minimising the intentional misuse of warning systems depends on improving the design of warning systems and promoting a positive warning culture, not on establishing sanctions against potential warners.

7. ***Should whistleblower protection measures include rewards or benefits?***

Establishing a system of monetary rewards or benefits for whistleblowers in the public interest may pose a greater risk to the functioning of the law. Although other countries, such as the United States of America, have established similar systems, we believe that this could be highly risky in Spain, and would go against the spirit of the law itself. Those who choose to report wrongdoing or malpractice should do so as a selfless act, in defence of the values of their community, discouraging a utilitarian understanding of whistleblowing.

The risks would be even greater if potential retribution were conditional on the recovery of assets from possible crimes identified and prosecuted as a result of whistleblowing.

At the same time, we do endorse the provision of financial support to whistleblowers, which is foreseen in the Directive. The experience of blowing the whistle can prove ruinously expensive, with a career-long impact on a whistleblower's earning potential (see, for example: https://www.whistleblowingimpact.org/post-disclosure-survival-strategies/#publications). An Independent authority might set aside a certain proportion of their budget for the purpose of supporting whistleblowers in legal proceedings, healthcare and other matters.

8. ***Finally, what other issues do you think should be considered in addition to the transposition of the Directive?***

The non-obligatory use of internal channels as a first option

A key aspect of the Directive is that whistleblowers are empowered to decide where to make their first report. There is no obligation to make an internal report first ("mandatory internal reporting"). Instead, whistleblowers must be able to make their report to the competent external authority or – in exceptional cases – to the broader public via the press.

It is recommended to provide specific mention of protection for whistleblowers who turn, either as a first or last option, to elected representatives, union officials, quality and safety bodies, and international bodies with a public interest role. This should not exclude other avenues however.

Access to information and legal consultation for whistleblowers

The transposition law should include provisions ensuring that whistleblowers have access to all the information they need to make an educated decision about making a report, in particular they need to be informed about the different available reporting channels, what is allowed to gather and secure the relevant information to make a report, which rights they have in case of, e.g., retaliation measures, which other consequences they may face and who to turn to in each case.

Therefore, it should, for example, be mandatory that the transposition law as well as information on the responsible individuals for handling reports shall be made public

in the respective company or office. Similarly, the authorities competent to receive reports should be mandated to provide the relevant information on their website and offer individual consults, and, where necessary, legal assistance.

Strict timelines for the processing of reports

The transposition law should provide for clear timelines for the processing if reports at both internal and external reporting channels. In accordance with recitals 57, 58 of the Directive informing, as far as legally possible and in the most comprehensive way possible, the reporting person about the follow-up to the report is crucial for building trust in the effectiveness of the overall system of whistleblower protection. This should occur no later than 3 months after the initial report was made.

While the Directive already envisages such timelines for the handling of reports itself, it is important that the transposition law includes similar provisions – albeit with shorter deadlines – for cases where whistleblowers seek legal support when they, for example, face reprisals from their employer (e.g. if they are being let go or discriminated in the work place). In such cases, the competent channel must be able and obliged to act quickly and implement preliminary measures where needed.

Extradition

We are increasingly concerned about the impact of extradition proceedings on freedom of expression and have noted an increasing number of extradition cases focused on journalists and whistleblowers. Extradition as an institution assumes good faith between states and often places a public interest value on the maintenance of the ongoing bilateral relationship, as opposed to individual rights.

Concerns have been expressed in recent years that extradition and related procedures are vulnerable to abuse. In particular, there has been some focus on the use of Interpol Red Notices. See for example the recent work of the Europea Parliament's DROI committee: https://op.europa.eu/en/publication-detail/-/publication/e124eaac-7078-11e9-9f05-01aa75ed71a1.

A related issue is the decline of the traditional exemption for political offences, particularly in bilateral and multilateral relationships where there is a high degree of assumed trust between legal systems (for example the European Arrest Warrant). Unfortunately, we see this has facilitated the use of extradition against whistleblowers and journalists, even within the EU.

Current examples include Rui Pinto (alleged source behind the "Football Leaks" disclosures), who was extradited from Hungary to Portugal in 2019.

British whistleblower Jonathan Taylor was detained in Croatia six months ago on the basis of extradition proceedings initiated by Monaco.

The case of WikiLeaks publisher Julian Assange has created concern in the UK about the decline in protection against politically-motivated extraditions (see, for example: https://hansard.parliament.uk/commons/2021-0121/debates/D907B179-BE6A-466E-B2AC-9B68D8808EE9/ExtraditionAct2003).

In recent years, several attempted extraditions of whistleblowers within the EU have been blocked, among them the cases of Maria Efimova and Herve Falciani. These cases cause hardship to whistleblowers, even if they are ultimately overturned.

The establishment of an Article 10 defence, or bar, to extradition would present more of a barrier to abuse of the system as it would dissuade abusive requests from being made.