Angel Castro-Rivera (*)
ABL Compliance Business Unit

THE DIRECTIVE (EU) 2019/1937 on the protection of "WHISTLEBLOWERS"[1]

On April 16th 2019 the European Parliament adopted, at the first reading, the Proposal for a Directive of the Parliament and of the Council on the protection of "Whistleblowers". During the last quarter of last year (23rd October 2019) this proposal was finally approved, with slight changes, through the DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on the protection of persons who report breaches of Union law (hereinafter: the Directive).

This Directive becomes an excellent model for all specialists who work within companies or governments located in the European Union (EU), or who are specialized in compliance issues.

Similarly; the Directive serves as a model tool for any professional or international company interested in the design of the so-called "reporting channels"; by establishing a set of common minimum standards to protect informants (from private and public companies); as well as any person who is linked to the infringing entity in the context of its labor activities. The breaches envisaged are of a diverse nature such as: public procurement; financial services, products and markets; prevention of money laundering; financing of terrorism; public health; consumer protection; protection of privacy and personal data.

The Directive seeks to establish sources of information to find out what is happening within the companies and to overcome the pitfall that arises by "not communicating" obvious infringements due to the lack of confidence (in the effectiveness of potential complaints) and the latent fear of possible reprisals against informants/whistleblowers. It is recognized that there is no better informant than the workers themselves (and all other persons with similar positions or links) as they are in a "privileged position" to report on any case of corruption, fraud, abusive practices or negligence. It is also accepted that, by not avoiding such threats, serious harm to the public interest may arise (including abuses of rights and all kinds of acts or omissions, which, without necessarily being unlawful, may frustrate the ultimate objective of the laws) .

From an entrepreneurial point of view, the implementation of the reporting channels set out in the Directive also serve to prevent and detect risky behaviors that are occurring within the companies and to provide an important self-assessment tool. Particularly , these reporting channels, serve as a fundamental part of the implementation of any adequate "compliance

[1] See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937&from=ES

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

system" aimed at achieving the exemption or mitigation that each national legislation grants by having implemented an effective and efficient "Compliance Management System" (CMS).

A special mention is deserved for the active role that the Directive gives to trade unions as a social interlocutor, counselor and unit of support for informants. The aforementioned proposal for a Directive of the European Parliament and of the Council of 16th April 2019, indicated that trade unions should be consulted on the internal procedures to be implemented, in order to facilitate the reporting of infringements. This proposal also mentioned that even the procedures to be established may be negotiated under collective agreements, and that trade unions themselves may act as recipients of the disclosures of informants. In this regard, Article 24 of the Directive is particularly relevant when it states that: *"the rights and remedies provided for under this Directive cannot be waived or limited, by any agreement, policy, form of employment, including a pre-dispute arbitration clause".*

Next, we will carry out a succinct analysis of the most important points of this Directive; as well as on the confidentiality protection measures; non retaliation of the informant; the use of internal, external and public disclosure channels among other topics that we consider of great interest to any employee, entity or person interested in delving deeper into the topic.

Scope of Application

The Directive applies to all "informants" who, working in the private or public sector, have learned of relevant infringements (provided that the access to that information does not constitute an offence itself, in which case the criminal liability will still be governed by the corresponding national law).

The aforementioned "labor context" includes all types of workers (salaried or not) and at least: workers in practice; shareholders and persons belonging to the management or supervisory body; contractors; subcontractors and suppliers in general, as well as informants who have identified infringements in the context of an already finished employment relationship or even in employment relationships not yet started (as in the case of an ongoing selection process, pre-contractual negotiation phases, volunteers and trainees).

Similarly, all types of "facilitators" (**natural persons** assisting the informant in a confidential manner and within a working context) are also included within the "protection spectrum"; as well as all third parties linked to the informant who may also suffer retaliation (i.e: friends, family, colleagues, etc.) and any **legal person** owned by or linked to the informant and who may face retaliation in a contractual context.

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

In essence, the position of economic vulnerability of the "informant or worker" and all of those directly related to him, is protected against the legal entity they depend upon (whether or not a remuneration or monetary compensation exists).

Role of the Member States

All EU member states must additionally:

- point out the competent authorities to receive and properly process the relevant complaints mentioned in the Directive . They must also ensure that these authorities review their procedures for the reception and processing of infringements with regularity.

- introduce or maintain provisions that are even more favorable to the informants' rights. The Directive, under analysis, only establishes the minimum framework for protection. This train of thought also makes it possible to demand that small companies (from specific sectors, and after the respective assessment) also establish the necessary channels to report possible infringements.

- establish "provisional and precautionary measures" to protect informants while they are awaiting the resolution of the judicial process.

Minimum protection standards

The minimum protection offered to "informants or workers [2] " must be:

- Prohibition of all types of direct or indirect retaliation (i.e. dismissals, degradation, negative references, job changes, cancellation of contracts for goods or services, refusal of training, discrimination, early termination of contracts, etc.).

- The provision of effective advice and legal assistance by the competent authorities, as well as access to corrective measures against retaliation and even remedies and full compensation for damages (i.e.: free legal aid, reversing the burden of proof in such a way that it is the employer who must prove that the harm suffered is not a consequence of the informant's actions, etc.). This type of support and assistance should be easily accessible and free of charge.

[2] It is important to note that, as regards the definition of 'worker', we use the interpretation of the Tribunal of Justice concerning paragraph 1, article 45 of the TFEU that considers workers : **all persons that during a period of time work for others or under their management in exchange for a specific compensation** . For more information see judicial sentences of the 3rd July 1986, Lawrie-Blum, Case 66/85; 14th October 2010, Union Syndicale Solidaires Isére, Case C-428/09; 9th July 2015, Balkaya, Case C-229/14; 4th December 2014, FNV Kunsten, Case C-413/13; 17, 2016, Ruhrlandklinik, Case C-216/15.

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

- The protection of professional secrecy, since it is expressly stated that the directive shall not in any way affect the protection of the prerogative of professional secrecy in the client-lawyer relationship and in other professions, in accordance with national law[3].

- The provision of financial assistance and support measures of various kinds (including psychological support), if required.

- Right to effective judicial protection, the right to defense, an impartial judge, the presumption of innocence and the free access to the informant´s judicial files.

- Protection of the identities of the informants and all the affected persons. For this purpose only authorized members or competent and trained personnel (specifically appointed to receive and process the given information through the respective channels) may have access to their identities and contact details[4].

Obligatory Implementation of Reporting Channels

In the private sector, it should be implemented in companies with 50 or more employees[5] (however, member states are expressly given discretion to demand it from companies with fewer workers when they consider it necessary if their activities could pose a particular risk to the environment and/or public health).

In addition, companies with 50 to 249 workers are allowed to share resources for the "reception of potential infringements and their investigation"; so as not to make it´s implementation so onerous in small companies.

Micro and small enterprises are exempt from this scope of application. It is established that "informants" working in such enterprises that wish to inform of infringements can do so directly through the external channels and/or to the competent national authorities. The exemption does not apply to micro and small enterprises operating in the field of financial services (susceptible to money laundering or financing of terrorism).

In the public sector, it must be implemented in any entity belonging to the state administration, including the regional and provincial administrations (in proportion to its size).

[3] This point is extremely relevant because there were initially many detractors in this regard, who argued that these types of infringements should also be communicated by professionals who learned about them through their clients (since general interest should prevail).

[4] Identity may only be disclosed when considered compulsory by national or Union Law to safeguard the right of defense of the person concerned.

[5] In the first proposal adopted on 16th of April of last year, the European Parliament spoke of companies with a turnover or annual balance sheet of 10 million euro or more.

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

It is established, however, that member states may exempt public entities and municipalities with fewer than 10,000 inhabitants or less than 50 workers. In small public entities that do not have internal reporting channels, these communications can be conducted through a higher level of the Administration (i.e. at the regional or central level).

Similarly, it is established that several municipalities may share internal "reporting channels" or agree that they will be managed by joint municipal authorities in accordance with national law, provided that these shared channels are clearly differentiated and independent of the external reporting channels.

Types of Channels and Main Characteristics

The Directive establishes 3 types of "whistleblowing" channels (internal , external and public disclosure), but in principle each private and public legal entity is free to choose the types of channels to make these communications effective (i.e. personal contact, by email, through a physical mailbox, by telephone, intranet or the Internet) provided that the necessary confidentiality is guaranteed [6].

(a) internal reporting channels:

are those established within the entities themselves (in both the private and public sectors) that enable the communication of infringements , verbally and/or in writing or even through a face-to-face meeting granted within a reasonable time.

The communication of infringements, through this type of channel, should be encouraged provided that they can be dealt with "effectively and without the risk of possible retaliation".

As a general rule the informant should receive feedback, within a 3 month timeframe, starting from the acknowledgement of its reception (or 7 days after submission if the respective acknowledgement was not made).

[6] There has been much debate as to whether the reporting channels should be "anonymous" or "confidential", but finally Article 6,2 of the Directive makes it clear that **there is complete freedom for member states themselves to accept or require anonymous or confidential infringement reports.**

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

b) external reporting channels:

are those means provided by the private or public entities that enable the communication confidentially, independently and, in particular, treated by a specialist outside the entity itself and with total autonomy.

The communication of infringements may be verbal or written and are used in cases where the internal reporting channels cannot reasonably be expected to function properly.

The main appeal of this type of channel, is that it greatly reduces the fear of communicating possible infringements, allowing total confidentiality and security when reporting alleged irregularities to someone outside the entity itself.

All EU member states shall designate which authorities shall be competent concerning the reception and treatment of possible infringements. These authorities must be independent and autonomous in all respects.

As a general rule, the informant should be promptly informed about the actions taken. Usually within 3 months after communicating the possible infringement or six months if the case demands it . They must give an acknowledgement of receipt 7 days after its reception, unless the informant requests otherwise or if this acknowledgement jeopardizes their identity.

In the case of shared channels, they shall be clearly differentiated from the ordinary channels of communication of the competent authorities and shall be published in a separate, easily identifiable and accessible section of their websites.

Main common features of both types of channel:

- Written complaints must be promptly acknowledged (maximum 7 days after receipt, unless the identity of the informant is compromised) and should be diligently monitored.
- The registration of complaints should be done in a durable and accessible format and should offer the possibility of checking, rectifying and accepting them.
- The integrity and confidentiality of the information provided must be ensured; as well as the identity of the informant and any of the aforementioned third parties.
- An impartial, trained and competent person or department shall be appointed to follow complaints and the access to this information must be restricted for unauthorized personnel.

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

- There is a duty of confidentiality so that the identity of the informant is not disclosed without their express consent (except in the case of investigations followed by national authorities or in the context of a judicial process).
- The applicable confidentiality regime must be clearly indicated. The informants must know in advance if their infringement reports will be treated confidentially or anonymously.
- Personal data and information must be treated under the data protection regulations of the European Union (EU Regulation 2016/679 and Directive 2016/680 and EU Regulation 2018/1725).
- It must be clearly explained that informants do not incur any kind of liability and that the infringements they report do not violate the restrictions on communication of information (imposed contractually or by any other legal provision).

(c) public channel or "public disclosure":

is referred to that path that remains open for cases that had already been reported (through the corresponding internal or external reporting channels) and which have not received the appropriate treatment within the due timeframe or in the cases that the infringement remains uncorrected . In these cases, the informants decide to make it public through web platforms, social media, elected officials, civil society organizations, trade unions or business or professional organizations. The cases disclosed to the press in the full exercise of freedom of expression and information are exempt.

This type of public disclosure is enabled when:

- The reported infringement may constitute an imminent or manifest danger to the public interest.
- There is a high risk of retaliation or there is a reduced chance of effective treatment of the already communicated infringement in the case of external channels.

Requirements and Safeguards against Malicious Reports

In order to be fully protected, informants must reasonably believe that the facts they have notified are truthful and they must have reasonable grounds to believe that the public disclosure was necessary.

Whistleblowers shall not be liable for the acquisition or access to the information that is publicly communicated or disclosed, provided that such acquisition or access does not in itself constitute an offense.

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .

As a general rule, sanctions and compensation are required to ensure the effectiveness of the whistleblower protection rules, but they are also applicable for whistleblowers who have reported a possible infringement by being aware of its falsehood . These measures seek to compensate for all unnecessarily suffered damages and expenses.

In order to preserve the credibility of the "whistleblowing system" established by this Directive, it is expressly stated that the protection system established shall not apply to those who knowingly and consciously report incorrect or misleading information.

This Directive should be transposed by EU member states by the 17th of December 2021. Private sector legal entities with 50 to 249 workers will have until the 17th of December 2023 to comply with the obligation of establishing internal reporting channels.

---.---

"Audere est Facere"
To Dare is to Do

(*)Angel Castro is a leading partner from MG ABOGADOS PERU and the ABL Compliance Business Unit Director and a certified Compliance Officer through IFCA, ASCOM/CESCOM and EQA. Currently he is a researcher for compliance in the public sector at the faculty of law in the Complutense University in Madrid, Spain .