Argentina – Whistleblowing

January 2022

1. LEGISLATION | NOTABLE CASE LAW

1.1. List any specific whistleblowing legislation

- Repentant Law, Law No. 27,304 of 2016 (only available in Spanish here) ('the Repentant Law')
- Complex Crimes Law, Law No. 27,319 of 2016 (only available in Spanish here) ('the Complex Crimes Law')
- Witness Protection Law, Law No. 25,764 of 2003 (only available in Spanish here) ('the Witness Protection Law')

1.2. List any sector-specific whistleblowing legislation

Not applicable.

1.3. List any additional applicable legislation

There are constitutional principles, as well as labour, and data privacy laws that provide certain guidelines for the implementation of whistleblowing programs. In this sense, the provisions of the following laws are applicable:

- Criminal Code, Law No. 11,179 of 1984 (only available in Spanish here) ('the Criminal Code');
- Personal Data Protection Act, Act No. 25,326 of 2000 ('the PDP Act');
- Decree No. 1558/2001 Regulating the PDP Act (only available in Spanish here);
- Labour Contract Law, Act No. 20,744 of 1976 (only available in Spanish here) ('the Labour Contract Law');
- Corporate Criminal Liability Law, Law No. 27,401 (only available in Spanish here) ('the CCL Law');
- Decree No. 62/2019 on Procedural Regime for Civil Forfeiture (only available in Spanish here) ('the Civil Forfeiture Decree');
- Antitrust Law, Law No. 27,442 of 2018 (only available in Spanish here) ('the Antitrust Law');[1] and
- regulations issued by the Argentinian data protection authority ('AAIP') may be applicable.

1.4. List any notable decisions. I.e. case law or decisions from supervisory authorities

Not applicable.

2. GUIDELINES

The Anti-Corruption Office ('the Anti-Corruption Office') has issued the Guidelines for the Implementation of Integrity Programs (only available in Spanish here) ('the Guidelines'), which clarify the extent of the provisions of the CCL Law. In particular, Section 3.5 of the Guidelines provides certain standards regarding internal reporting channels, and Section 3.6 covers the protection of whistleblowers.

3. OVERVIEW

3.1. Outline the legislative protection for whistleblowing

The Witness Protection Law created the National Witness Protection Program in 2003.

The program sets forth several protection measures, including:

- personal or domiciliary custody;
- temporary accommodation in reserved places;
- change of address;
- provision of economic means for lodging, transportation, food, communication, health care, moving, labour reintegration, and other essential expenses (although not for more than six months).

In addition to complementing the protective-oriented measures, positive incentives to whistleblowers have also been established by legislation. On the one hand, the Repentant Law foresees that persons investigated for corruption and other complex crimes (except high ranking State officials) may obtain a reduction of their punishment and the avoidance of a prison sentence during the process in exchange for the disclosure of precise, useful, and verifiable information relating to other participants in the offence and who occupied a higher hierarchical role in the criminal organisation. The Repentant Law has been effectively applied and has provided great visibility to the anti-corruption agenda, especially in the context of a case known in Argentina as 'the Notebook Case,' in which multiple businessmen

and former public officials reached cooperation agreements, boosting the investigations. The Repentant Law makes the Witness Protection Program applicable to whistleblowers. Similarly, the Complex Crimes Law allows 'informants' to provide information and documentation related to organised crime to the police and other law enforcement agencies in exchange for a reward (Article 13 of the Complex Crimes Law).

When it comes to corporate internal whistleblowers, the CCL Law encourages companies to establish a procedure for internal reporting so that employees and third parties can file reports anonymously and without fear of retaliation (Article 23(c)(III) and (IV) of the CCL Law).

Additionally, the Antitrust Law provides that any person who has committed or is in the process of committing any of the offences listed in Section 2 of the Antitrust Law may disclose and acknowledge such conduct before the Competition Tribunal in exchange for an exemption or reduction of the sanctions set forth in the Antitrust Law. However, it is worth noting that the aforementioned Competition Tribunal has not been created yet, and the Secretary of Domestic Trade has not regulated the operative details of its leniency program. Therefore, there are no clear rules on how the whistleblowers' protection framework will be enforced yet.

In addition, and according to the Property Decree, which sets a procedural regime for civil action, the Public Prosecutor's Office ('MPF') may develop collaboration programs with the persons who provide relevant information for asset recovery proceedings. The collaborating persons may be awarded up to 10% of the goods obtained as a consequence of the information they provide.

3.2. Outline the whistleblowers who are protected under the law. E.g. workers, agents, etc.

In order to enjoy whistleblower protection under the Witness Protection Law, the individual must be either charged for the crimes provided by law or act as a witness.

Under the Repentant Law, the individual must be an author or contributor to the crimes set forth in Article 1 of the Repentant Law.

Under the Complex Crimes Law, as mentioned above, an informant shall be any person who provides relevant information to police authorities in order to initiate or guide the investigation regarding a crime listed in the Complex Crimes Law.

Concerning corporate whistleblowing, the Guidelines establish that reporting channels have to be properly accessible to all employees as well as to third parties and related parties (e.g. vendors, suppliers, and business partners). However, the implementation of whistleblower protection programs is not mandatory for companies.

In order to enjoy the benefits set out in Article 60 of the Antitrust Law, the person reporting the conduct must have performed or be currently performing the action prescribed.

3.3. What kind of disclosures or actions are protected under the law? – internal or external reporting?

Both internal and external reporting actions are covered by law, depending on each regulation (see sections 3.1. and 3.2. above).

3.4. Is legal protection limited to certain subject matters? E.g. criminal offences, health and safety.

The Witness Protection Law, the Repentant Law, and the Complex Crimes Law only allow whistleblowing in criminal investigations for certain serious offences (e.g. the sale of narcotics, customs crimes, insider trading, money laundering, terrorism financing).

The CCL Law limits whistleblowing for some corruption offences (e.g. bribery, trading in influence, illicit enrichment) (Article 1 of the CCL Law).

Finally, the Antitrust Law allows whistleblowers for antitrust offences only (e.g. agreements of any kind between two or more competitors), having the following purpose or effect (Section 2 of the Antitrust Law):

- fixing, directly or indirectly, the selling or purchase price of goods and services that are offered or requested in the market;
- imposing obligations to:
    - produce, process, distribute, purchase, or market only a restricted or limited amount of goods; and/or
    - supply a restricted or limited number, volume, or frequency of services;

- horizontally distributing, dividing, allocating or imposing zones, market shares or segments, supply clients or sources; or
- establishing, agreeing on or coordinating bids, or the non-participation in bid processes, tenders or auctions.

3.5. What information do employees have to be provided with about a whistleblowing scheme?

The Guidelines establish that internal corporate policies should clearly inform employees about the company's sanctioning regime, and the general internal investigation procedure. If the company undertakes or implements surveillance activities (e.g. via telecommunications, email, video surveillance, etc.), employees should be clearly informed that they should have no expectation of privacy.

4. NOTIFICATION, REGISTRATION AND APPROVAL OF WHISTLEBLOWING SCHEMES

4.1. Is prior notification/registration with the data protection authority or any other body, such as a works council required? If so, how must this notification/registration be made?

The PDP Act does not require notifying the AAIP in order to implement a whistleblowing program. However, if the whistleblowing program includes the creation of a database containing employees' or other data subjects' personal data, the company must register such a database with the AAIP. Moreover, regardless of the existence of a formal database, as every whistleblower scheme implies the processing of personal data, it will be necessary to comply with the requirements set forth in the PDP Act.

4.2. Is prior approval of the scheme by the data protection authority or any other body, such as a works council required? If so, how must this approval be sought?

No, prior approval is not required. However, the AAIP could be consulted as an advisory body to ensure compliance with the PDP Act. Additionally, it should be noted that the AAIP

often initiates *ex officio* investigations and companies should be prepared for such a scenario.

These procedures must comply with several rights and guarantees provided in the Constitution of the Argentine Nation (only available in Spanish here) ('the Constitution'), the Labour Contract Law, and the PDP Act.

In addition, the Guidelines establish that if a company decides to conduct an internal investigation, it is essential that the investigation process respects employees' rights to intimacy, privacy, and dignity.

5. MANAGEMENT OF WHISTLEBLOWING SCHEMES

5.1. What are the specific internal organisational requirements for the management of a whistleblowing scheme?

The CCL Law establishes that corporations may conduct internal investigations with due respect to the rights of the persons under investigation, and imposes effective sanctions in case of violations to the internal policies or applicable laws (Article 23(c)(V) of the CCL Law).

Furthermore, the Guidelines establish that if a company decides to conduct an internal investigation, it is essential that the investigation process observes the limits arising from employees' rights, namely their privacy and dignity (Articles 70 and 72 of the Labour Contract Law). Information management must comply with the rules on gathering and handling personal information (Section 43 of the Constitution). There must be a balance between the right to investigate and the protection of privacy and dignity.

In addition, the Guidelines establish that it is important that internal investigations respond to a written internal protocol previously approved by the board of directors, and previously communicated and agreed with the potential investigated persons in the form of a written agreement. Such an agreement must include allowing the company to access the sources and devices provided to the employees to perform their work. Employees must be warned about the fact that information stored in such sources or devices is the property of the

corporation, and that no privacy is to be expected in the event that these are used for personal or illicit purposes.

The Guidelines also set up an investigations protocol, regulating areas such as the chain of custody of the gathered information, how electronic evidence should be handled, and witness interviews, among others.

The procurement of outside counsel to conduct the investigation is advisable, especially when the allegations involve senior management, are particularly serious, or may have severe reputational consequences. Retaining outside counsel contributes to strengthening the independence and the credibility of the investigation process as well, and enhances attorney-client privilege.

In any case, it should be noted that internal investigations are a new feature in Argentine domestic law. The current state of case law is quite unbalanced in favour of employees due to Argentina's robust labour and data privacy protections.

5.1.1. With whom does the responsibility lie for the management of the scheme?

According to the CCL Law, the responsibility for the management of the scheme lies with an internal officer of the company that implements it.

5.1.2. Does a separate department isolated from the HR department have to be created?

It is not mandatory, but the Guidelines encourage companies to do so.

5.1.3. Are there any specific hotline requirements? E.g. multilingual approach.

The Guidelines provide that the internal report channels must be safe, and organisations must assure complainants that the information will be kept strictly confidential and will only be used for serious and professional analysis or investigation. These channels shall be open to third parties and adequately publicised.

5.2. Is it possible to use external service providers? If so, what obligations and liabilities are imposed on the external service providers?

Yes, it is possible to use external service providers when conducting internal investigations. The Guidelines recommend this in cases in which members of the boards of directors are involved in the facts under investigation.

Additionally, and pursuant to Article 25 of the PDP Act, the outsourcing of data processing services shall be performed by means of a written data processing agreement foreseeing certain requirements. This means that data cannot be applied or used for any purpose other than that foreseen in the agreement, nor can such data be communicated to other parties, even for storage purposes.

Once the corresponding contractual obligations have been performed, the processed personal data must be destroyed. In addition, the processor must comply with the PDP Act and the complementary rules dictated by the AAIP, and the data processor must not subcontract processing services.

Further requirements, related to international data transfers, may apply if the service provider is located in a foreign country and, according to the AAIP, if such country does not have an adequate level of data protection. A list of all adequate countries can be found in Regulation No. 34/2019 of the AAIP (only available in Spanish here).

Additional sector-specific regulations may impose further requirements (e.g. banking and financial sector).

6. ANONYMITY OF WHISTLEBLOWERS

6.1. Is anonymous whistleblowing permissible? If so, in what circumstances and are there any special precautions required?

Anonymous reporting lines have been opened in recent years by the Economic Crime and Money Laundering Prosecutor's Office ('PROCELAC') and the Prosecutor's Office for Administrative Investigations ('PIA') both at the MPF and by the Anti-Corruption Office.

Moreover, different administrative agencies have opened anonymous reporting lines, such as the Argentine Internal Revenue Service ('AFIP') and the National Food Safety and Quality Service ('SENASA').

When it comes to corporate internal whistleblowers, the CCL Law encourages companies to establish a procedure for internal reporting so that employees and third parties may file reports anonymously and without fear of retaliation (Article 23(c)(III) and (IV) of the CCL Law).

6.2. Does the confidentiality of reports made through whistleblowing schemes have to be guaranteed? If yes, are there any exceptions to this guarantee?

It is not mandatory, but the Guidelines highlight that confidentiality should be guaranteed. The Guidelines also encourage companies to set clear rules regarding when exceptions to confidentiality would take place (e.g. government investigations).

Pursuant to Section 60(d) of the Antitrust Law, the Competition Tribunal shall keep the identity of the whistleblower confidential. Furthermore, the declarations, acknowledgements information and/or any other means of evidence that had been submitted to the Competition Tribunal cannot be disclosed.

7. RIGHTS OF THE ACCUSED

7.1. Does the person accused in a whistleblower's report have to be informed when data concerning them is recorded? Please state any time limits.

The Labour Contract Law does not contain any provision in relation to this matter. Nevertheless, following case law, employers may apply a precautionary suspension to suspend an employee during an internal investigation, as long as the investigation is still ongoing. Please be aware that employees under investigation may choose not to cooperate since they are not obliged to testify against themselves or to confess misbehaviour. Therefore, and according to general labour law principles, in case of a trial, a confession may not have any legal value.

In certain cases, depending upon the gravity of the facts under investigation, it is advisable to request the employee explanations on the case, even when this is not a legal requirement to proceed with a dismissal.

It should also be noted that Article 7 of the PDP Act establishes that the data subjects have a right to be informed about any processing operations of their personal data. However, this right could be limited by the data controller during an investigation, on the grounds of the legitimate interest to conduct the investigation in an efficient manner. After the investigation has ended, regardless of its results, the data controller would have to notify the data subject that was previously under investigation and let them know about the details of the processing of their personal data.

7.2. What information must the person be made aware of? E.g. the entity responsible for the whistleblowing scheme, the actions they are accused of and related facts.

In line with the answer above, the employee should be provided with the information necessary for them to prepare a defence (mainly, the actions they are accused of and the relevant evidence).

7.3. Does the accused have a right to have their identity remain confidential? I.e. beyond those involved in the investigation.

It should be noted that under Argentine law, everyone must be presumed innocent until proven guilty. Therefore, depending on the circumstances, disclosing the accused's identity may expose the company to liability.

From a strictly data protection standpoint, the general confidentiality obligation set forth under Article 10 of the PDP Act would apply.

Regarding the Antitrust Law, as noted above, the whistleblower's identity and any information submitted to the Competition Tribunal regarding the accused shall remain confidential.

7.4. Does the accused have a right to access, rectify and erase their data?

Under the PDP Act, all data subjects have a right to access, rectify or erase any information related to them. However, these rights could be limited by the data controller during an investigation, on the grounds of the legitimate interest to conduct the investigation in an efficient manner.

After the investigation has ended, the data controller should reassess whether it must comply with the data subject's requests. Depending on the circumstances, there could be a legitimate interest or a legal obligation to retain the personal data and preserve it from erasure or modification.

7.5. What legal recourse is available for the accused?

On one hand, data subjects who want to enforce their data protection rights can present claims before the AAIP. On the other hand, Article 33 of the PDP Act regulates the *habeas data* action a judicial remedy available to any data subject seeking enforcement of their data protection rights. These two recourses are simultaneously available and it is not necessary to use one before the other.

Other specific labour remedies may also apply.

8. PENALTIES

8.1. Please outline any penalties for failure to notify/unfair dismissal/unlawful detriment

In case the employer terminates an employee through a dismissal for fair cause that is later considered by a labour court to be without cause or in the event of a constructive dismissal duly decided by the employee, the employer will be obliged to pay the severance package plus applicable fines. It is highly probable that, in case of an internal investigation, the employee opts to terminate the labour relationship through a constructive dismissal alleging different labour infringements. In order to avoid this, once the internal investigation is over and depending on its conclusions, employers may decide to terminate the labour

relationship with the employee through a dismissal without cause, paying them the corresponding severance compensation package.

8.2. May an organisation face other kinds of liability? E.g. Is there vicarious liability for retaliation by co-workers?

It will depend on the measures adopted during the investigation. For instance, access to employees' emails, messages and other content in their computers might be considered an invasion of the employee's privacy rights and therefore, they could claim the cessation of such actions and eventually, if the employer does not cease them, the employee could consider themselves dismissed and claim, from the employer, the payment of the severance compensation package.

Moreover, Article 153 of the Criminal Code sanctions, with imprisonment from 15 days to one year, anyone who unduly opens, accesses, or seizes an electronic communication. Additionally, Article 153 bis of the Criminal Code sanctions whoever knowingly accesses by any means and with no authorisation or exceeding it, a computer system or data of restricted access with 15 days to six months imprisonment.

The PDP Act provides for the following administrative sanctions:

- written warnings;
- suspension of the database;
- cancellation of the database; and
- pecuniary fines depending on the nature of the infringement.

The PDP Act also foresees specific criminal sanctions, including prison terms ranging from one month to two years for:

- illegitimate access to a database;
- illegitimate disclosure of information stored in a database; and
- illegitimate insertion of data in a database or file (Articles 117 bis and 157 bis of the Criminal Code).

The unauthorised disclosure of personal data of any individual or entity will result in the obligation of the offender to compensate the data subject for the damages caused by the infringement. Please note that Argentine law recognises two sorts of damages: economic loss and moral distress.

The application of vicarious liability would depend on the circumstances of the specific case and the court's interpretation.

8.3. Please outline any compensation that is available to whistleblowers. E.g. monetary/reinstatement

The Complex Crimes Law allows the possibility to offer economic awards to whistleblowers (Article 13 of the Complex Crimes Law).

Under the Property Decree, for persons who collaborate in an asset recovery procedure, compensation may reach up to 10% of the amount of the recovered assets (Article 18 of the Property Decree).

The National Witness Protection Program sets forth several protection measures, including the provision of financial means for accommodation, transport, food, communication, health care, relocation, reintegration into employment, formalities, security systems, housing arrangements and other essential expenses, within or outside the country, for as long as the beneficiary is unable to obtain them by his own means. In no case shall financial assistance be granted for more than six months.

Under the Antitrust Law, whistleblowers that have committed any anti-competitive behaviour provided therein shall obtain a reduction or be exempted from penalties established in the Antitrust Law, and from the prison sentences that may be applicable to them in any case for having committed any of the offences set forth in Sections 300 and 309 of the Criminal Code.

1. Please note that on 4 February 2021, the Argentine Senators Chamber approved a bill by means of which, among other modifications, the whistleblowing program and the cease of conduct agreements would be repealed. The bill is yet to be discussed by the Chamber of Deputies, and the date for the debate is undefined.
2. 
3. **Guillermo Jorge**

4. *Bruchou, Fernández Madero & Lombardi*

5. Guillermo Jorge is an internationally recognised expert in anti-corruption compliance and money laundering prevention, highlighted by his clients for his sharp design of creative strategies to mitigate compliance risks.

6. Who's Who Legal recognised him as Global Elite Thought Leader 2018. In addition to frequently advising multinational and local companies, he is consulted in the processes of reform of integrity, anti-corruption and anti-money laundering public policies in Argentina and in most of Latin American countries, as well as by different international organisations such as the World Bank, the Inter-American Development Bank, the United Nations, the Organization of American States and the OECD.

7. guillermo.jorge@bruchou.com

8. 

9. Fernando Basch

10. *Bruchou, Fernández Madero & Lombardi*

11. Fernando Basch stands out in the handling of criminal law and corporate governance, integrity and compliance. He is consulted by companies and international organisations such as the World Bank, the Inter-American Development Bank, the United Nations Development Program and the World Economic Forum PACI Initiative. Fernando also led the collective remediation strategy of the Maritime Anti-Corruption Network (MACN) in Argentina.

12. Who's Who Legal 2018 recognised him as an expert consultant and praised his knowledge in criminal law and anti-corruption. Fernando is a senior researcher at the Center for Anti-Corruption Studies and an Associate Professor of the Master's in Business Law at the University of San Andrés, and a professor of Economic Criminal Law at the Master of Law at the University of Palermo.

13. fernando.basch@bruchou.com

14. 

15. Gabriel Lozano

16. *Bruchou, Fernández Madero & Lombardi*

17. Gabriel Lozano is a partner in the General Corporate and M&A Department of Bruchou, Fernandez Madero & Lombardi and leads the firm's Competition & Antitrust Law Department. His practice focuses primarily in mergers and acquisitions, and competition and antitrust law.

18. Prior to joining Bruchou, Mr. Lozano was the General Counsel of Syngenta in LAS (Argentina, Chile, Bolivia, Paraguay and Uruguay) from 2015 to 2018. Among other things, his daily practice included providing legal advice in contentious matters, contracts, data protection, trademarks and patents, and labour and regulatory law.

19. In 2020 Gabriel was elected President of the Competition Defense Commission of the Colegio de Abogados de la Ciudad de Buenos Aires.

20. gabriel.lozano@bruchou.com

21. 

22. Dolores María Cedrone

23. *Bruchou, Fernández Madero & Lombardi*

24. Dolores obtained a law degree with honours from the Law School of the Universidad Austral in 2016 and completed a postgraduate diploma in Private Law at the same university.

25. Dolores joined the firm in 2015 as a member of the firm's General Corporate and M&A Department, and of the Competition & Antitrust Law Department. Her practice focuses on mergers, acquisitions and general corporate matters, in addition to her experience in the renewable energy field. She also advises companies on competition and antitrust matters.

26. dolores.cedrone@bruchou.com

27. 

28. Manu Hersch Garcia

29. *Bruchou, Fernández Madero & Lombardi*

30. Manú Hersch Garcia is a lawyer, graduated summa cum laude from the University of Buenos Aires (2018). He currently works as a teaching assistant in the Department of Philosophy of said

university and previously collaborated as an assistant student in Corporate Law and Constitutional Law.

31. He advises multinational corporations, high net worth individuals and governments in anti-corruption and anti-money laundering compliance, as well as in white collar crime matters.

32. Manu.garcia@bruchou.com