United Nations A/HRC/55/46

General Assembly

Distr.: General
18 January 2024
English
Original: Spanish

Human Rights Council
Fifty-fifth session
26 February–5 April 2024
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Legal safeguards for personal data protection and privacy in the digital age

Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères

Summary

This report examines personal data protection and privacy laws from five continents with the aim of providing States with a comparative study of the different mechanisms that have been established so that data subjects can exercise control over the use of their personal data. It also examines the legal mechanisms that are available to data subjects for the protection and restitution of their rights and, where necessary, for the reparation of damage caused by the improper use of information concerning them.

I. Introduction

1. Human beings have always been an end in themselves: they are the raison d'être of States and of national and international society.[1]

2. Fundamental rights are the highest principles of any legal system. States must set out and establish the conditions and the necessary framework for the recognition and effective enjoyment of these rights in any space or territory where human beings are active or present.

3. The law must always be an effective means for treating human beings as an end in themselves. All persons, both governors and governed, and in all contexts, whether physical or virtual, must pursue their full realization.

4. As far as the Human Rights Council is concerned, the United Nations High Commissioner for Human Rights has already recognized that the right to privacy is an expression of human dignity and is linked to the protection of autonomy and personal identity.[2]

5. The Global Privacy Assembly has recognized that the rights to privacy and data protection buttress democratic processes. It has also observed that robust data protection laws place a reasonable limit on various negative situations, such as intrusive government influence on private life, undue external influence, data profiling, automated decisions and discrimination, which technologies such as artificial intelligence can amplify.[3]

6. The Joint Statement on Privacy and Democratic Rights, signed by the Office of the Privacy Commissioner of Canada and the Special Rapporteur on the right to privacy,[4] recognizes that the rights to privacy and personal data protection specifically and mutually support equality and democratic values and provide a guarantee for the respect of other fundamental rights and freedoms.

7. The digital age, regardless of the great benefits it brings for the development of humanity, must not diminish the rights and dignity of human beings.

8. At the 45th session of the Global Privacy Assembly, held in 2023, privacy authorities recognized that developments in technology, innovation and digitalization lead to new activities and business models which increasingly rely on processing of large volumes of personal data in new and progressively more complex ways.[5] They also noted that the exchange of data by States and individuals and various forms of data processing are increasing daily through the use of technologies whose capacities are growing exponentially and dynamically.

9. Privacy authorities also expressed concern that certain technological developments can pose new challenges for the implementation of data protection and privacy laws and can cause significant negative effects, such as discriminatory and biased outcomes for individuals, or affect their ability to exercise their data protection and privacy rights. This concern is particularly acute in relation to more intrusive processing of personal data, including sensitive data, especially those of children and vulnerable people.[6]

10. In this context, data subjects find themselves in a position of defencelessness owing to their limited knowledge of the use that third parties make of information concerning them, since in practice they are unable to follow up on or monitor this use. This has repercussions for their ability to control their data – the essence of the fundamental right to personal data protection.

[1] Universal Declaration of Human Rights.
[2] A/HRC/48/31, para. 7.
[3] See https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf.
[4] See https://priv.gc.ca/en/opc-news/speeches/2023/js-dc_20231208/.
[5] See https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf.
[6] Ibid.

11. In principle, States have a direct positive role to play in ensuring that rights and freedoms do not lose their essential content in the course of activities carried out in various sectors and by individuals.

12. It is necessary for States to establish a system to safeguard the right to personal data protection so that data subjects are aware of the processing to which their personal data are subjected, can exercise proper control over their data and, in the event of a violation, can opt for a remedy with a view to the reparation or restitution of the right or compensation for the damage caused, as the case may be.

13. In the digital age, not only must State respect and refrain from violating the rights to privacy and data protection, but their obligations also include positive measures to promote the effective enjoyment of these rights.[7]

14. The mere recognition of a legal standard on the right to personal data protection does not guarantee the effectiveness or enjoyment of that right without the existence of an accessible and effective protection system. Such protection systems are usually composed of a set of administrative and judicial remedies and, in some cases, alternative means of dispute resolution.

15. To safeguard their dignity, human beings must have sufficient means and mechanisms at their disposal to be able to assert their rights before those responsible for processing their personal data and various governmental bodies. The effectiveness of these rights is directly related to the existence of instruments that ensure their exercise.

16. To achieve the stated goal, States should, among other measures, establish an appropriate legal and regulatory framework, including suitable laws and regulations.

17. As the member authorities of the Global Privacy Assembly have recognized, jurisdictions across the world are increasingly enacting new privacy and personal data protection laws, and reviewing older ones, often building on similar elements.[8] It has also been noted that, given the variety of jurisdictions and legal systems, data protection and privacy laws differ in their approach and details, although they also present common traits.

18. This report contains an analysis of five data protection and privacy laws from five continents. The aim is to identify and compare the measures defined in each law so that data subjects can exercise control over the use of their data, be aware of the legal mechanisms available to them for the protection and restitution of their rights and, if necessary, seek reparation for damage caused by the improper use of information concerning them.

19. The analysis is structured so that each thematic point is accompanied by a comparative table on the content of the relevant laws.

20. The judicial institutions and their characteristics identified in the analysis are those established in the relevant data protection and privacy laws, without prejudice to the existence of other mechanisms that may be recognized in other bodies of law or provisions that do not form the basis of this report.

21. The continents, countries and laws chosen as the object of this study are:

- Oceania: Australia
    - The Privacy Act 1988[9]
    - The Australian Privacy Principles (APPs)[10]
- The Americas: Ecuador

[7] A/HRC/39/29, para. 23.

[8] See https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf.

[9] See https://www.legislation.gov.au/Details/C2023C00130.

[10] These are principles (and rights) that are annexed to and referenced in the Privacy Act of 1988. They are a cornerstone of personal data regulation in Australia. As the Principles have their own numbered articles, they are referenced in this analysis as a separate law.

- Organic Act on Personal Data Protection[11]

- Europe: Spain[12]
  - Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[13]
  - Organic Act No. 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights[14]
- Asia: Singapore
  - The Personal Data Protection Act[15]
- Africa: South Africa
  - Protection of Personal Information Act[16]

II. Rights of data subjects

22. Processing of personal data must be carried out respectfully and in accordance with a series of principles and requirements, thus ensuring that it is done properly while guaranteeing privacy and the unhindered development of personality, among other rights.[17]

23. To achieve this goal, data subjects must be able to exercise control over their personal information, which is why data protection and privacy laws grant them a number of rights.

A. Right of information

24. The right to information is the right of all data subjects whose data have been collected to obtain from the data controller certain information about the context and circumstances of the processing.

25. All of the laws considered in this analysis provide for this right, as can be seen in the comparative table (table 1) below, with the exception of that of Singapore, which considers it an obligation of the data controller.[18]

26. The timeliness with which the information is provided, the amount of data disclosed and the medium and form used are all important for the effective enjoyment of this right.

[11] See https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf (in Spanish).

[12] In the case of Spain, two laws have been considered for the following reasons. Direct implementation of the European Union regulation, which has been in force since 25 May 2018, is mandatory in the countries of the European Union. Spain was thus required to draft a new Organic Act in order to adapt its legal system to the European regulation. As its preamble explains, the purpose of Organic Act No. 3/2018 is twofold: firstly, to adapt the Spanish legal system to the European Union regulation and to supplement its provisions, on the understanding that the fundamental right of natural persons to personal data protection must be exercised in accordance with the European Union regulation and the Act; and, secondly, to guarantee the digital rights of citizens.

[13] See https://www.boe.es/doue/2016/119/L00001-00088.pdf (in Spanish).

[14] See https://www.boe.es/eli/es/lo/2018/12/05/3/con (in Spanish).

[15] The Personal Data Protection Act of Singapore applies to the private sector and does not cover the processing of personal data in the public sector. See https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?DocDate=20210930.

[16] See https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf.

[17] See A/77/196.

[18] Section 20 of the Personal Data Protection Act (“Notification of purpose”) provides that, before personal data are collected, used or disclosed, the controller must inform the individual of the purpose of doing so. It must also provide the contact information of an individual who is able to answer the data subject’s questions.

27. The laws of Australia, Ecuador, South Africa and Spain make a distinction as to whether the data was collected directly from the subject or from another source. Likewise, in Australia and Spain, there is a difference in the information that is provided, depending on its source.

28. In Australia, Ecuador, South Africa and Spain, the law stipulates when such information must be provided. These laws, except that of Australia, distinguish between data collected from the subject (in which case, information must be provided prior to or at the time of collection) and data collected from another source (information must be provided as soon as possible, within one month, or at the time of the first communication, depending on the country).

29. In Ecuador and Spain, the law provides that the information must be provided to the data subject in clear and simple language. The data controller must take appropriate steps to provide the information to the data subject in a concise, transparent, intelligible and easily accessible form. Ecuadorian legislation specifies that the presentation of information must be clear, precise, unequivocal and without technical barriers.

30. In the countries analysed, the data controller generally must provide information on:

- The purpose of the processing
- The legal basis for the processing and the identity and contact information of the data controller
- The existence of any data transfers or disclosures that it intends to make
- The consequences for the data subject of submitting or refusing to submit personal data
- The existence of rights and how to assert them
- The right to file a complaint with the supervisory authority
- The period of time for which the data will be retained

31. Under some countries' legislation, information must be provided on aspects such as the possibility of withdrawing consent; the existence of automated decision-making, including profiling, and information about the logic involved; and categories of personal data.

B. Right of access

32. By virtue of the right of access, data subjects can obtain from the data controller confirmation of whether their personal data is being processed and can gain access to such data and to certain information on how they have been used or disclosed. All of the laws considered in the analysis provide for this right.

33. In principle this right is exercised free of charge, although the laws of some countries (Australia, South Africa and Spain) mention that a reasonable fee may be charged in certain cases.

34. In Australia, access may not affect certain rights of third parties. In Spain, the right to obtain a copy of the personal data must not adversely affect the rights and freedoms of others.

35. Some laws establish exceptions to the right of access. This is the case in Singapore, when the provision of the information could cause grave harm to the safety or the physical or mental health of the data subject; in South Africa, when it might interfere with the Promotion of Access to Information Act; and in Australia, when it might prejudice law enforcement activities by an enforcement body.

C. Right to rectification

36. By virtue of this right, data subjects may obtain the rectification of inaccurate or incomplete personal data so that it reflects their actual situation. The Australian and South

African laws also refer to out-of-date, irrelevant or misleading data. All of the countries covered by the analysis provide for the right of rectification.

37. Data controllers must notify any corrections to all parties to whom the personal data has been disclosed, with certain exceptions.

38. Spanish legislation also provides for the right to rectification on the Internet, which includes a requirement for data controllers of social media and equivalent services to adopt appropriate protocols to allow the exercise of the right to rectification against users who disseminate content that violates the right to honour and personal and family privacy on the Internet. Controllers attending to requests for rectification must also publish a warning, in a visible place next to the original information, clarifying that the original news item does not reflect the individual's current situation.

D. Right to update information in digital media

39. This right is foreseen only in Organic Act No. 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (Spain). It empowers any person to request controllers of digital media, on a justified basis, to include a warning of an update in a visible place next to a news item concerning him or her and which does not reflect his or her current situation due to circumstances that have arisen since publication, causing him or her prejudice. This right applies in particular to cases where the original information refers to police or judicial proceedings and the data subject has benefited from a subsequent judicial decision.

E. Right to deletion

40. Data subjects have the right to have their personal data erased in certain circumstances. This right implies the obligation of the data controller to delete them.

41. The laws considered in the analysis provide for the deletion of data:

(a) When they have been unlawfully processed;

(b) When they have served the purpose for which they were collected or processed;

(c) When the retention period has ended;[19]

(d) When their processing undermines fundamental rights or individual liberties;[20]

(e) When consent is withdrawn or has not been given for one or more specific purposes and there is no other legal ground for the processing;

(f) To comply with a legal obligation.

42. All of the countries envisage exceptions whereby the request for deletion should not be carried out, such as where processing is necessary for the establishment, exercise or defence of legal claims, for the exercise of the right to freedom of expression and information, for compliance with a legal obligation or for the performance of a task carried out in the public interest.

43. In Spain and South Africa, the data controller must communicate any deletion of personal data to each recipient to whom they have been disclosed, unless this proves impossible or would require a disproportionate effort.

F. Right to be forgotten

44. Spain is the only country, of those analysed, whose law makes reference to the right to be forgotten, in connection with the right to deletion under Regulation (EU) No. 2016/679.

[19] Australia, Ecuador, Singapore and South Africa.

[20] Ecuador.

Organic Act No. 3/2018 regulates the right to be forgotten in Internet searches and social media and equivalent services.

45. The right to be forgotten in Internet searches implies that, after a search is carried out based on a person's name, search engines will remove from the list of results any published links that may contain data related to that person that is inappropriate, inaccurate, irrelevant, out of date or excessive, or has become so, or when the affected party invokes personal circumstances to justify the prevalence of his or her rights over the maintenance of the links by the Internet search service.

46. This right does not entail the deletion of the information, nor does it prevent users from gaining access to online information using search criteria other than the person's name.

47. The right to be forgotten in social media and equivalent services is the right of individuals to obtain the deletion of any personal data they may have provided for publication on social media.

48. This right entails the erasure of the person's data on the grounds that they are inappropriate, inaccurate, irrelevant, out of date or excessive or have become so due to the passage of time, or when the personal circumstances of the affected party justify the prevalence of his or her rights over the maintenance of the data.

49. In the event that the person exercising the right is doing so in relation to data provided when he or she was a minor, the service provider must delete the data without delay at the simple request of the data subject.

G. Right to restriction of processing

50. Of the countries analysed, only Ecuador and Spain have legislated to recognize this rights. In Ecuador it is called the "right to suspension of processing".

51. By virtue of this right, data subjects can obtain from the data controller the restriction of processing of their personal information when any of the following conditions are met:

(a) The accuracy of the personal data is contested, for a period enabling the controller to verify their accuracy;

(b) The processing is unlawful and the data subject opposes the deletion of the personal data and requests the restriction of their use instead;

(c) The controller no longer needs the personal data, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) The data subject has objected to the processing by virtue of the right to object, in Spain, or has objected to the processing of health-related data, in Ecuador; in both cases pending verification of whether the legitimate grounds of the controller override those of the data subject.

52. Where the processing of personal data has been restricted in accordance with this right, such data may, with the exception of storage, be processed only with the data subject's consent or for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of important public interest.

H. Right to data portability

53. Data subjects have the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit them to another controller, in certain cases.

54. They also have the right to have their data transmitted directly from one controller to another, where technically possible. Of the countries studied, this right has been established only in Ecuador and Spain.[21] It is applicable where:

(a) The processing is based on consent;

(b) The processing is carried out by automated means;

(c) The processing based on a contract (in Spain);

(d) There is a significant volume of personal data or the processing is necessary for compliance with obligations and the exercise of rights by the data controller, processor or subject in the area of labour and social security law (in Ecuador).

55. Spain also regulates the right to data portability in social media and equivalent services.

I. Right to object

56. This right is established in all of the countries considered. Its purpose is to ensure that data are no longer processed if an objection is expressed. In Australia and South Africa the right is regulated specifically in the sphere of marketing.

57. Data subjects have the right to object, at any time, on grounds relating to their particular situation, to the processing of their personal data.

58. Some laws, including those of Spain and Ecuador, establish exceptional circumstances in which data controllers do not have to accede to the request in which the objection is raised, such as when the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

59. If the purpose of the processing is direct marketing, data subjects have the right to object at any time and their personal data must no longer be processed for such purposes (Australia, Ecuador, South Africa and Spain). The Ecuadorian and Spanish laws also cover profiling.

J. Right not to be subject to a decision based on automated processing, including profiling

60. This right is regulated in Ecuador, South Africa and Spain.

61. All data subjects have the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them, and to express their position.

62. The laws of Ecuador, South Africa and Spain provide for exceptions to this right, for example, if the decision is necessary for the conclusion or performance of a contract by the data subject or if it is authorized by an applicable law which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests.

63. In Ecuador and South Africa, data subjects may request the controller to provide a reasoned explanation of the decision taken and information on the evaluation criteria of the automated program; they may also make observations. Ecuadorian law provides that data subjects cannot be required to relinquish this right in advance in standard form contracts.

64. In Ecuador, the law makes specific provision for children and adolescents, whose data may not be processed without the express authorization of their legal representative, unless

[21] In Singapore, the right to data portability does not yet exist. Section 48H (1) of the Personal Data Protection Act currently provides that if portability obligations are not respected within a reasonable time, data subjects may file a complaint with the Personal Data Protection Commission. Section 26H of the Personal Data Protection (Amendment) Act of 2 November 2020, which is not yet in force, would recognize this right.

the data subject is aged 15 years or older or the processing is intended to safeguard an essential public interest.

K. Right to a digital will

65. Of the countries considered, only Spain has a law that regulates this right, which allows data subjects to decide what will happen to content managed by information society service providers upon their death. Thus, they can decide whether their personal profiles on social media and equivalent services should be maintained or deleted and whether certain persons should be prevented from accessing their content or requesting its modification or deletion.

Table 1
Legal recognition of the rights of data subjects

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
	Privacy Act/Australian Privacy Principles (APPs)	Organic Act on Personal Data Protection	Regulation (EU) No. 2016/679 or Organic Act No. 3/2018	Personal Data Protection Act	Protection of Personal Information Act
Right of information	APP 5	Art. 12	Regulation (EU) (Personal data collected from the data subject), art. 13 Regulation (EU) (Personal data not obtained from the data subject), arts. 12 (1), (5) and (7) and 14 Organic Act No. 3/2018, art. 11		Sect. 18
Right of access	APP 12	Art. 13	Regulation (EU), art. 15 Organic Act No. 3/2018, art. 13	Sect. 21	Sect. 23
Right to rectification	APP 13	Art. 14	Regulation (EU), arts. 16 and 19 Organic Act No. 3/2018, arts. 14 and 85 (the latter covers the right to rectification on the Internet)	Sect. 22	Sect. 24
Right to update information in digital media			Organic Act No. 3/2018, art. 86		
Right to deletion	APP 11	Art. 15[22]	Regulation (EU), art. 17 Organic Act No. 3/2018, art. 15	[23]	Sect. 24

[22] In Spanish, "*derecho de eliminación*" (right of elimination).

[23] The Personal Data Protection Act makes no provision for the right to deletion as such. However, under section 25, "Retention of personal data", data controllers must cease to retain personal data or remove the means by which personal data can be associated with particular individuals when the purpose for which they were collected is no longer being served or when retention is no longer necessary for legal or business purposes. Section 16 (4) provides that the withdrawal of consent is another reason for ceasing to retain personal data.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Right to be forgotten			Regulation (EU), art. 17 Organic Act No. 3/2018, art. 93 (covers Internet searches) Organic Act No. 3/2018, art. 94 (in social media and equivalent services)		
Right to restriction of processing		Art. 19	Regulation (EU), arts. 18 and 19 Organic Act No. 3/2018, art. 16		
Right to data portability		Art. 17	Regulation (EU), art. 20 Organic Act No. 3/2018, art. 17 Organic Act No. 3/2018, art. 95 (covers portability in social media and equivalent services)		
Right to object	For marketing APP 7.6	Art. 16	Regulation (EU), art. 21 Organic Act No. 3/2018, art. 18	Sect. 16	For marketing Sect. 69 (2) and (3)
Right not to be subject to a decision based on automated processing, including profiling		Arts. 20 and 21[24]	Regulation (EU), art. 22 Organic Act No. 3/2018, art. 18		Sect. 71[25]
Right to a digital will			Organic Act No. 3/2018, art. 96		

66. The laws of all five countries expressly recognize the various rights of data subjects. Some countries are moving forward by legislating to recognize new rights, such as those that are linked to automated and digitalized processing or are exercised online or on social media. This progress can also be seen from the more detailed express recognition of certain rights.

III. Exercise of rights by data subjects

67. Data subjects exercise their rights vis-à-vis data controllers through procedures that are regulated by each legal system. Various aspects of these procedures are described below.

68. It is for the data controller or, where appropriate, the data processor, to attend to rights requests. The laws of Ecuador, South Africa and Spain refer to "the responsible party". In Australia, the name used varies and encompasses a broader concept than that of data controller; reference is made to the "APP entity", meaning a public-sector agency or

[24] The decision may be based solely or partially on automated assessments. Article 21 refers exclusively to the right of children and adolescents.

[25] A data subject may not be subject to a decision which results in legal consequences for him or her or which affects him or her to a substantial degree, which is based solely on the automated processing of personal information intended to provide a profile of such person.

private-sector organization. In Singapore, the law refers to an "organization", which has competence for the processing of personal data only in the private sector.

69. In all of the countries analysed, the person authorized to exercise rights is the data subject. In some countries, the law provides expressly for the possibility of representation and, specifically, the representation of minors. Spain is the only country of those studied in which the law defines the medium of response, as can be seen in table 2.

70. All of the countries envisage different ways of responding to rights requests. In Australia and Spain, the law provides that if the data subject's request is refused, he or she must be informed without delay of the reasons for the failure to act and of the possibility of lodging a complaint with a supervisory authority and of seeking a judicial remedy. In Singapore, the refusal must be based on legal grounds.

71. All of the laws examined, except that of Singapore, establish a time limit for the data controller to respond, which varies substantially from one country to the next. Indeed, this deadline ranges from the earliest possible moment to 10 days to one month. In the case of South Africa, with respect to the rights to correction and deletion, a response should be provided as soon as is reasonably practicable.

72. The laws of Australia, Ecuador and Spain provide that the exercise of rights vis-à-vis the data controller must be free of charge. However, the Australian and Spanish laws provide for the possibility of fees in certain cases. In South Africa, in respect of the right of access, fees for providing information are at the controller's discretion, but must be reasonable.

Table 2
Exercise of rights before the data controller

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
	Privacy Act/Australian Privacy Principles	Organic Act on Personal Data Protection	Regulation (EU) No. 2016/679 or Organic Act No. 3/2018.	Personal Data Protection Act	Protection of Personal Information Act
Name of data controller	APP entity (sect. 6)	Controller (art. 4)	Controller (Regulation (EU), art. 4 (7))	Organization (sect. 2)	Responsible party (sect. 1)
Person authorized to exercise rights	Data subject (APP 5)	Data subject (art. 62) Minors, either through their representatives or directly if aged 15 years or older (art. 24)	Data subject or his or her legal representative Minors under 14 years old through persons exercising parental authority (Organic Act No. 3/2018, art. 12).	Data subject (sects. 16, 17 and 21–22A)	Data subject (sect. 23) Minors, through their representatives (sect. 35 (3))
Verification of the data subject's identity			Regulation (EU), art. 12 (6)		Sect. 23
Medium of response			In writing or by other means, or orally, if requested (Regulation (EU), art. 12 (1) and (3))		

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Form of response	In principle, access must be given to the information, and it must be corrected (APP 12.1 and 13.1). If the entity refuses the request, it must communicate the reasons for the refusal, the mechanisms available to complain and any other matter prescribed by the regulations (APP 12.9 and 13.3).	Affirmative or negative (art. 62)	The information must be provided (Regulation (EU), art. 12 (3)) If the controller does not take action on the request, it must inform the data subject of the reasons and of the possibility of lodging a complaint with the supervisory authority and of seeking a judicial remedy (Regulation (EU), art. 12 (4) and Organic Act No. 3/2018, art. 12)	The request may be processed or rejected on various grounds (sects. 21 and 22).	The data controller may refuse the request in certain circumstances (sect. 23)[26]
Deadline for responding	As soon as possible, with regard to the right of information (APP 5) On request by the data subject, in respect of the right to object, the right to deletion and the right of access (APPs 7, 11 and 12) 30 days, in case of correction, if the controller is an agency, and as soon as possible, if it is an organization (APP 13.5)	10 days after the request is submitted (art. 62)	Within one month of receipt of the request, extendable by two further months (Regulation (EU), art. 12 (3))		As soon as is reasonably practicable, in the case of correction and deletion (sect. 24 (2))
With or without charge	Free of charge Exception: a small charge may apply if the controller is an organization (APP 12.7 and 12.8)	Free of charge (art. 62)	Free of charge Exception: manifestly unfounded or excessive requests (Regulation (EU), art. 12 (5) and Organic Act No. 3/2018, art. 12)		For the right of access, it is free to confirm whether the controller holds the subject's information. A reasonable fee may be charged for providing the data (sect. 23)

73. All of the countries studied have regulated aspects of the procedure for the exercise of rights by the data subject before the data controller. Regulated aspects include the medium of response; whether or not a fee is charged for the procedure; the duty to inform the data subject, in the event of refusal of the rights request, of the possibility to file a complaint with an administrative or judicial authority; and the deadline for responding to requests.

[26] There are circumstances in which the data controller may refuse to provide access to personal data. For example, if there is a fee for the service of providing the data to the data subject, the controller may refuse to provide the service until the fee is paid. Another example established by law is where providing access would contradict the Promotion of Access to Information Act.

74. Several of these aspects, as recognized in the text of the laws, are seemingly intended to better ensure the protection of rights.

IV. Legal mechanisms to ensure the effective enjoyment of rights

75. Legal recognition of the rights of data subjects is only the first step towards achieving the effective protection of individuals and their rights and dignity.

76. Legal recognition alone is not enough, as these rights are often ignored, disregarded or not respected. The problem is exacerbated in cases that involve the use of emerging technologies such as artificial intelligence, which can have considerable adverse effects for individuals, both in the present and the future, bearing in mind that technological advances should not entail their losing control over information that concerns them.

77. If a right is infringed owing to a failure or refusal to protect it, the situation must be remedied as soon as possible. For this reason, it is necessary for States to establish a framework of administrative and judicial remedies that are accessible to affected persons, with the aim of ensuring the timely protection, reparation and restitution of rights.

V. Administrative protection mechanisms

78. The laws of Australia, Ecuador, Singapore, South Africa and Spain establish an administrative supervisory authority in the area of data protection and privacy.

79. Data subjects may turn to this administrative authority in the event that the controller fails or refuses to protect their rights. In this way, the State affords the necessary protection.

80. Countries have different names for the supervisory authorities and the actions that may be brought before them.

81. In Australia, complaints are brought before the Privacy Commissioner.

82. In Ecuador, administrative complaints are filed with the Personal Data Protection Authority.

83. In South Africa, complaints must be submitted to the Information Regulator.

84. In Singapore, the procedure is to apply for a review by the Personal Data Protection Commission.

85. In Spain, complaints must be filed with the Spanish Data Protection Agency, although autonomous regional authorities may take action in certain cases.[27]

86. In terms of standing,[28] the laws of Australia, Ecuador, Singapore and Spain[29] establish that data subjects have the right to bring an action. Australian law provides that when there are several affected parties, any data subject may take action.

87. In South Africa, complaints may be lodged by a data subject, any person alleging interference with the personal information of a data subject, any person with sufficient personal interest or any person acting in the public interest.[30]

88. Both Ecuadorian and South African legislation provides for the representation of minors, differentiating by age group in the case of Ecuador.

89. In Spain, the law provides that not-for-profit bodies, organizations or associations may lodge complaints where mandated by a data subject or where the State provides for them to

[27] Organic Act No. 3/2018, art. 57.

[28] Capacity to act as applicant or plaintiff.

[29] The data subject is termed the *interesado* (interested party) in the Spanish text of Regulation (EU) No. 2016/679 and the *afectado* (affected party) in Organic Act No. 3/2018.

[30] See https://inforegulator.org.za/wp-content/uploads/2020/07/20211012-InfoReg-RulesOfProcedure-HandlingPOPIAcomplaints.pdf, rules 4.1.3 and 4.1.5.

do so and they consider that the rights of the data subject have been infringed as a result of the processing of personal data.

90. The laws of all five countries provide for the need to turn to the data controller before seeking administrative protection, although in Australia this step may not be necessary in some cases.

91. The admissibility of administrative proceedings varies from one country to the next. In Ecuador, Singapore and Spain, administrative action may be taken when rights requests are not attended to in a timely manner; in Australia, when there has been interference with an individual's privacy; and, in South Africa, when the data controller has violated the data subject's rights or when an unfavourable decision is handed down by the adjudicator in an arbitration process established under the controller's code of conduct.

92. As to whether complaints to the supervisory authority are free of charge, Spain is the only country where this is the case. Australian law does not specify, but there are indications that charges apply in some cases.[31]

93. Spain is the only country to set a time limit for resolving the administrative procedure.

94. Ecuadorian law provides that the Personal Data Protection Authority may open preliminary proceedings ex officio or at the request of the data subject in order to determine the specific circumstances of the case and whether it is advisable to initiate the administrative procedure.

95. In Australia, South Africa and Spain, the supervisory authority may, before taking any further action, examine its own competence. If it considers that it is not competent, it may refer the complaint to the appropriate authority.

96. In the same countries, the authority must assess whether the complaint is admissible in the light of the circumstances.[32] Once the complaint has been admitted, preliminary investigative proceedings may be conducted in order to better determine the facts and circumstances that justify the procedure.[33]

97. In Australia, the supervisory authority may in some cases restructure different aspects of the complaint in order to better achieve a better resolution of the issue.

98. Australia, Singapore and South Africa establish the possibility of referring the matter to an alternative dispute resolution mechanism as a preliminary measure.

99. Possible decisions – ways in which the authority may resolve the case – are set forth in the laws of all the countries considered, except Ecuador.

100. In Australia, Singapore, South Africa and Spain, the authority may close the case. In Spain, the complaint may be considered upheld if the authority does not respond by the established deadline.

101. In South Africa, if the Information Regulator ultimately decides to impose penalties or other measures, it may seek the advice of the Enforcement Committee, a consultative body.[34] The Regulator may also publish its decisions in full or in part.

102. All of the laws studied provide for measures to protect the right claimed in the complaint, as can be seen in table 3.

103. Under the laws of Australia and Ecuador, the supervisory authority may order measures to prevent the continuation of the infringement or the repetition of the conduct, regardless of any administrative penalties that may apply.

[31] Privacy Act, sects. 38A (2) (a) and 52.

[32] In South Africa, Protection of Personal Information Act, sect. 77 (1) (b); in Spain, Organic Act No. 3/2018, art. 65.

[33] Organic Act No. 3/2018, art. 67.

[34] The Enforcement Committee is a consultative body of the Information Regulator comprised of 14 independent members from different professional backgrounds. See https://inforegulator.org.za/wp-content/uploads/2020/07/Media-Statement_Information-Regulator-Establishes-Enforcement-Committee.pdf.

104. In all countries, the authorities can order measures such as the cessation of processing, the deletion of data or compliance with the request.

105. Australia is the only country where the authority, the Privacy Commissioner, may require an entity under investigation to engage an independent adviser to review the situation and provide a copy of the review to the Commissioner. It may also require the entity to prepare and publish a statement about its conduct.

106. Only the laws of Australia and Singapore provide for the possibility of appealing against the authority's decisions before a higher administrative body. In both cases, the law specifies the types of decision that may be subject to appeal.

107. In the laws of Australia, Singapore, South Africa and Spain, administrative protection against violations of the right to personal data protection and privacy is supplemented by the possibility of challenging the decisions of the administrative authority before the courts, in accordance with the right to effective judicial protection, as can be seen in table 3.

Table 3
Administrative protection mechanisms

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
	Privacy Act/Australian Privacy Principles	Organic Act on Personal Data Protection	Regulation (EU) No. 2016/679 or Organic Act 3/2018	Personal Data Protection Act	Protection of Personal Information Act
Action taken before the supervisory authority	Complaint (Privacy Act, sect. 36)	Administrative complaint (art. 64)	Complaint (Regulation (EU), art. 77)	Review (sect. 48H)	Complaint (sect. 74)
Supervisory authority	Privacy Commissioner	Personal Data Protection Authority	Spanish Data Protection Agency	Personal Data Protection Commission	Information Regulator
Standing	The data subject If there are several affected data subjects, any of them (Privacy Act, sect. 36) Action may be taken by a representative (Privacy Act, sects. 36 (2A) and 38 (1)).	The data subject (art. 64) Minors, either through their legal representatives or directly if aged 15 or older (art. 24)	The data subject (Regulation (EU), art. 77) The affected party (Organic Act No. 3/2018, art. 63) An entity, organization or association[38] mandated by the data subject or (if the State provides for its right to lodge a complaint) which considers that the data subject's rights have been infringed (Regulation (EU), art. 80)	The data subject (sect. 48H)	Any person (sect. 74)[39] In the case of children, a competent person such as a parent or legal guardian (sect. 35 (3))

[38] The not-for-profit body, organization or association must have statutory objectives which are in the public interest and be active in the field of the protection of data subjects' rights and freedoms.

[39] The Protection of Personal Information Act provides for the Information Regulator to take action in cases of "interference with the protection of the personal information of a data subject" (sect. 73), which includes situations other than the violation of the data subject's rights.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Need to take action before the data controller first	Yes However, in certain cases the Commissioner may decide that it is not necessary (Privacy Act, sect. 40 (1A) and (1B)).[40]	Yes (art. 64)	Yes (Organic Act No. 3/2018, art. 64 (1))[41]	Yes (sect. 48H)	Yes (sect. 74)[42]
Admissibility	When there is interference with an individual's privacy (Privacy Act, sect. 36 (1))[43]	When there is no response within the deadline or the request is denied (art. 64)	When the request has not been attended to (Organic Act No. 3/2018, art. 63)	When a request for the protection of the rights recognized under sections 21 and 22 has been refused (sect. 48H)[44]	When there has been a rights violation or an unfavourable decision is handed down by the adjudicator in an arbitration process established under the controller's code of conduct (sect. 74)
With or without charge	Not specified There are indications that charges apply in some cases		Free of charge (Regulation (EU), art. 57 (3))		
Deadline for a decision			Three months to decide on admissibility and then six months from notification of admissibility (Organic Act No. 3/2018, arts. 64 and 65). Preliminary investigative proceedings, if any, may not last longer than 18 months (Organic Act No. 3/2018, art. 67).		

[40] Section 40 (1A) of the Act does not give reasons why it may not be necessary. The Office of the Commissioner describes certain circumstances on its website. Section 40 (1B) relates to cases concerning access to and the correction of credit reporting information.

[41] The requirement is assumed "where the procedure refers exclusively to a failure to respond to a request to exercise the rights set forth in articles 15–22 of the Regulation (EU)" (Organic Act No. 3/2018, art. 64 (1)).

[42] For the authority to take action, it is necessary for there to have been "interference with privacy", the possible causes of which may include the data controller's refusal of a request for the exercise of rights.

[43] In relation to the rights of data subjects, "interference with the privacy of an individual" is defined as breach of the Australian Privacy Principles or of a code of practice binding an APP entity with a data subject.

[44] Sections 21 and 22 refer to the rights of access and correction, respectively.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Preliminary proceedings	The Commissioner may: • Attempt to conciliate the complaint (Privacy Act, sect. 40A) • Decide not to investigate (Privacy Act, sect. 41) • Conduct preliminary inquiries (Privacy Act, sect. 42) • Require information or documents (Privacy Act, sect. 44) • Hold a mandatory hearing with any person (Privacy Act, sects. 43, 43A and 45–47) • Refer the matter to other authorities (Privacy Act, sect. 50) • Restructure the complaint for the better resolution of the issue (Privacy Act, sects. 38A–38C)	The Authority may open preliminary proceedings ex officio or at the request of the data subject to determine whether it is appropriate to initiate the administrative procedure (art. 63)	The Agency may: • Decide whether to admit the complaint (Organic Act No. 3/2018, art. 65) • If it considers that it is not the principal authority, refer the complaint to the authority it deems competent, closing the case (Organic Act No. 3/2018, art. 66)	The Commission may: • Refer the matter to an alternative dispute resolution mechanism (sect. 48G)	The Regulator may: • Reject the complaint (sect. 76) • If it considers that it is not the appropriate supervisory authority to decide, refer the case to the appropriate authority (sect. 78). • Before investigating, it must inform the data subject, the complainant and any other aggrieved persons that an investigation will be opened and provide details (sect. 79)[45] • Refer the case to mediation without investigating (sect. 80)
Possible decisions of the authority	It can dismiss the complaint or find it substantiated and take various measures (Privacy Act, sect. 52)		It can close the proceedings at any time if the data controller or processor demonstrates that it has taken measures to comply with the rules (Organic Act No. 3/2018, art. 65) Six months after the notification of admissibility, the data subject can consider the complaint to have been upheld (Organic Act No. 3/2018, art. 64)	It can confirm, reject or modify the measure that gave rise to the complaint by the data subject (sect. 48H) If the data controller does not take action to comply with the Commission's decision, the latter may give specific	The Regulator can choose from a wide variety of options and may decide to take no action (sect. 77) It can impose penalties and other measures and may be advised by the Enforcement Committee (sects. 80 and 89–92)

[45] In South Africa, investigations may be conducted not only into violations of the rights of data subjects but also in the event of violations of data protection principles and in other circumstances. It is therefore possible that the Information Regulator may have to notify an affected party that is neither a data subject nor a complainant.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
				directions (sect. 48I)	
Measures to protect the right claimed	Yes (Privacy Act, art. 52)[46]	Yes (art. 65)[47]	Yes (Regulation (EU), art. 58 and Organic Act No. 3/2018, art. 69 (3))[48]	Yes (sect. 48J)[49]	Yes (sect. 95)[50]
Appeals	Certain of the Commissioner's decisions may be reviewed by the Administrative Appeals Tribunal (Privacy Act, sect. 96)			Administrative appeals may be lodged with the Appeal Panel (sect. 48Q)[51]	
Possibility to challenge administrative decisions before the courts	Proceedings may be brought before the Federal Court or the Federal Circuit and Family Court of Australia in order to enforce a decision of the Commission (Privacy Act, sect. 55A (1))		There is a right to an effective judicial remedy against a legally binding decision of a supervisory authority (Regulation (EU), art. 78)	Appeals may be lodged with the General Division of the High Court (sect. 48R)	There is a right to appeal to the High Court against the Regulator's decisions (sect. 97)

VI. Judicial protection mechanisms

108. States that have personal data protection and privacy laws usually establish a legal framework consisting not only of administrative remedies, but also judicial ones, in order to strengthen the protection of fundamental rights such as the right to personal data protection and privacy.

109. Of the laws studied here, those of Ecuador and Spain provide for judicial proceedings. In both cases, it is clarified that it is not necessary to first initiate administrative proceedings – that is, to turn to administrative supervisory authority – in order to take legal action before the courts.

110. It is for the data subject, as the affected party, to decide whether to turn to the administrative supervisory authority, as discussed in the previous chapter, or to approach the

[46] Measures include ordering the entity to take specific steps to prevent future privacy violations. The entity may also be required to prepare and publish a statement about their conduct. The Commissioner can require an entity under investigation to engage an independent adviser to review the situation and provide a copy of the review to the Commissioner.

[47] "Corrective measures" may include the cessation of the processing and the deletion of data.

[48] Organic Act No. 3/2018 provides for the obligation to protect the claimed right (art. 69), while Regulation (EU) No. 2016/679 provides for supervisory authorities to have the following corrective powers: (a) to order compliance with requests for the exercise of rights (art. 58 (2) (c)); (b) to order that processing operations be brought into compliance with the provisions of the Regulation (art. 58 (2) (d)); (c) to impose a limitation, including a ban, on processing (art. 58 (2) (f)); (d) to order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed (art. 58 (2) (g)); and (e) to order the suspension of data flows to a recipient in a third country or to an international organization (art. 58 (2) (j)).

[49] Measures include directions: (a) to stop collecting, using or disclosing data; (b) to destroy data; and (c) to comply with any previous directions (sect. 48J).

[50] Responsible parties may be required to take the specified steps within a specified period or to refrain from taking them. They may also be required to stop processing certain information (sect. 95).

[51] The Appeal Panel is an independent body that decides appeals against the Commission's decisions.

competent judicial body in order to seek a remedy for the protection of personal data that the data controller has failed to protect.

111. In Ecuador, data subjects may, in parallel with administrative proceedings, pursue any constitutional remedies to which they may consider themselves entitled. In Spain, the law provides for the right to a judicial remedy, without prejudice to any other administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority. It is therefore understood that administrative proceedings do not have to be initiated or completed in order to begin legal action before the courts.

112. In Ecuador and Spain, standing to take legal action is that of the data subject.

113. Regarding the courts before which action can be taken, Spanish legislation provides that the competent courts are those of the European Union member State that fulfils the conditions outlined in table 4. In the case of Ecuador, the case is referred to the competent judge, but the law does not set out the procedure in this regard.

Table 4
Judicial protection mechanisms

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
	Privacy Act/Australian Privacy Principles	Organic Act on Personal Data Protection	Regulation (EU) No. 2016/679 or Organic Act No. 3/2018	Personal Data Protection Act	Protection of Personal Information Act
Standing		The data subject (art. 64)	Each data subject (Regulation (EU), art. 79)		
			A not-for-profit entity, organization or association mandated by the data subject or (if the State provides for its right to lodge a complaint) which considers that the data subject's rights have been infringed (Regulation (EU), art. 80)		
Admissibility			When a data subject considers that his or her rights under the Regulation have been infringed (Regulation (EU), art. 79)		
Court before which proceedings are brought			The courts of the European Union member State where the controller or processor has an establishment or where the data subject has his or her habitual residence (Regulation (EU), art. 79)[52]		

[52] Unless the controller or processor is a public authority of an European Union member State.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Party against whom proceedings may be brought			A data controller or processor (Regulation (EU), art. 79) or a representative thereof (Organic Act No. 3/2018, art. 30)		
Requirement to initiate administrative proceedings before turning to the courts		No, constitutional remedies may be pursued in parallel (art. 64)	No, judicial proceedings are without prejudice to any other administrative or non-judicial remedy (Regulation (EU), art. 79)		

VII. Redress mechanisms

114. Any person who has suffered damage as a result of a breach of personal data protection and privacy laws should be able to obtain redress for the prejudice incurred. To this end, he or she should pursue the remedies afforded by the legal system. All five countries regulate certain aspects of redress to a greater or lesser extent.

115. There are differences in the names given to the action that must be taken. In Ecuador, the law provides for "civil action"; in Spain, for "court proceedings for exercising the right to receive compensation"; in Singapore, for the "right of private action"; and, in South Africa, for "civil remedies". Australian law does not name any specific action.

116. In terms of standing, Ecuador and South Africa establish that data subjects may institute proceedings. In South Africa, the data subject may also request the Regulator to act on his or her behalf. In Australia, the Commissioner has standing to commence proceedings, although data subjects may also do so where the Commissioner has issued an administrative decision in their favour.

117. In Spain, standing extends to any person, in addition to the data subject, who may have suffered material or non-material damage as a result of an infringement of Regulation (EU) No. 2016/679. Data subjects have the right to mandate a body, organization or association that meets certain requirements to exercise the right to receive compensation on their behalf.

118. All the laws analysed, with the exception of that of Ecuador, contain provisions establishing capacity to be sued.[53] The laws of South Africa and Spain refer to the data controller in this regard, while the Spanish law also includes data processors and representatives and provides in certain cases for joint and several liability for damage caused in order to ensure the effective compensation of data subjects.

119. In Australia and Singapore, capacity to be sued lies with the APP entity and the organization that caused the damage, respectively. These entities encompass notions broader than those of data controller and data processor.

120. In Australia, redress may be sought for any loss or damage, including injury to feelings and humiliation. Spanish law refers to material and non-material damages; South African law to patrimonial and non-patrimonial loss; and Singaporean law to loss or damage.

121. In Australia, the competent court may be the Federal Court or the Federal Circuit and Family Court. The laws of Ecuador, Singapore and South Africa provide only for a civil action or civil proceedings to be brought before a competent court or tribunal. According to

[53] Lies with the party that is required to fulfil an obligation.

Spanish law, proceedings may be brought before the courts competent under the law of the European Union member State that fulfils the conditions outlined in table 5.

122. The legislation of Singapore, South Africa and Spain expressly establishes a causal link between the infringement and the damaging outcome. In Spain, any person who has suffered damage as a result of an infringement of Regulation (EU) No. 2016/679 has the right to receive compensation. Singaporean law stipulates that any person who suffers loss or damage as a result of a contravention has a right to relief. In South Africa, the law states that loss suffered as a result of a breach of the provisions of the Protection of Personal Information Act will give rise to action against the responsible party.

Table 5
Redress mechanisms

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
	Privacy Act/Australian Privacy Principles	Organic Act on Personal Data Protection	Regulation (EU) No. 2016/679 or Organic Act No. 3/2018	Personal Data Protection Act	Protection of Personal Information Act
Name of the action		Civil action (art. 64)	Court proceedings for exercising the right to receive compensation (Regulation (EU), art. 82 (6))	Right of private action (sect. 48O)	Civil remedies (sect. 99)
Standing	The Commissioner, or the data subject based on a decision of the Commissioner (Privacy Act, sect. 55A)	The data subject (art. 64)	Any person[54] who has suffered damage as a result of an infringement of the Regulation (Regulation (EU), art. 82)	The person who has suffered loss or damage (sect. 48O)[55]	The data subject or, at the data subject's request, the Regulator (sect. 99)
Capacity to be sued	Person or entity (Privacy Act, sect. 55A)[56]		Data controllers and processors[57, 58] (Regulation (EU), art. 82 (2)) and representatives (Organic Act No. 3/2018, art. 30), with joint and several liability (Regulation (EU), art. 82 (4)) A properly constituted[59] not-for-profit body, organization or association, mandated by the data subject (Regulation (EU), art. 80 (1))	The organization that caused the loss or damage (sect. 48O)	The responsible party (sect. 99)

[54] "Any person" being a broader notion than "data subject".

[55] In the event that administrative proceedings are ongoing before the supervisory authority, action may not be brought until after the decision has become final.

[56] Including APP entities (agencies or organizations).

[57] "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller (Regulation (EU) No. 2016/679, art. 4 (8)).

[58] Data controllers and processors are liable for damage caused by processing that does not comply with Regulation (EU) No. 2016/679.

[59] Whose statutory objectives are in the public interest and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

	Australia	*Ecuador*	*Spain*	*Singapore*	*South Africa*
Type of damage for which redress may be claimed	Any loss or damage (Privacy Act, sect. 52), including: • Injury to feelings • Humiliation (Privacy Act, sect. 52 (1AB))		Material or non-material damage (Regulation (EU), art. 82 (1))	Loss or damage (sect. 48O)	Patrimonial and non-patrimonial loss (sect. 99)
Cause of the damage			An infringement of the Regulation (Regulation (EU), art. 82 (1))	A contravention of the Act (sect. 48O)	A breach of any provision of the Act as referred to in section 73 (sect. 99)[60]
Competent court	The Federal Court or the Federal Circuit and Family Court (Privacy Act, sect. 55A (1))		The courts of the European Union member State where the controller or processor has an establishment or where the data subject has his or her habitual residence (Regulation (EU), art. 82 (6))[61]	Civil proceedings in a court (sect. 48O)	Civil action in a court (sect. 99)
Expression of a causal link between the infringement and the damaging outcome			Yes Damage as a result of an infringement of the Regulation gives rise to the right to receive compensation (Regulation (EU), art. 82 (1))	Yes When the loss or damage is suffered directly as a result of a contravention (sect. 48O)	Yes Loss suffered as a result of a breach of the provisions of the Act (sect. 99)

VIII. Conclusions

123. **The following conclusions can be drawn from this analysis:**

(a) **Countries from five continents have expressly recognized in their legislation the different rights that data subjects enjoy and that allow them to control their personal information. Eleven rights were identified in the legislation of the countries analysed;**

(b) **Some countries are moving forward by legislating to recognize new rights, including those that are linked to automated and digitalized data processing or are exercised in the context of the Internet or of social media and similar services. This progress can also be seen from the more detailed express recognition of certain rights;**

(c) **Data subjects exercise personal data protection rights vis-à-vis data controllers through regulated procedures in each legal system that possess similarities and particular features;**

[60] Section 73 defines “interference with the protection of the personal information of a data subject”, which includes the violation of his or her rights.

[61] Unless the controller or processor is a public authority of a member State acting in the exercise of its public powers.

(d) **Regulated aspects of these procedures include, depending on the law in question, the ability of the data subject or his or her representative to submit requests for the exercise of a right; the types of possible response; the medium of the response; the deadline for responding; whether the procedure is free of charge; and, if a rights request is refused, the duty to inform the data subject of the possibility of submitting a complaint to an administrative or judicial authority;**

(e) **In respect of administrative remedies, which data subjects may pursue if the data controller fails or refuses to protect their rights, there is a degree of regulatory convergence. The laws of certain countries include specific provisions on the submission of complaints free of charge; on time limits for the resolution of procedures; and on the possibility of referral to alternative dispute resolution mechanisms;**

(f) **In all of the laws considered, provision is made for administrative measures to protect the claimed right; some of which are intended to prevent the continuation of the infringement or repetition of the conduct;**

(g) **Certain laws clearly establish the possibility of appealing against the decisions of the supervisory authority before a higher administrative body and the possibility of challenging the decisions of the supervisory authority before the courts in accordance with the right to effective judicial protection;**

(h) **In some countries, the law gives data subjects the option of whether to turn to the administrative supervisory authority or to directly approach the competent judicial body in order to seek a remedy for the protection of personal data that data controller has refused or failed to protect;**

(i) **The five countries covered by the analysis regulate, to a greater or lesser extent, aspects of the redress that may be sought by data subjects who have suffered damage or loss as a result of a breach of data protection and privacy legislation. However, only one country provides for the joint and several liability of data controllers, processors and representatives.**

IX. Recommendations

124. **In the light of the foregoing, the Special Rapporteur urges States to:**

(a) **Establish and bring up to date appropriate legal frameworks, on a multidisciplinary basis and with the support of all stakeholders, in particular through the adoption of laws and regulations that provide accessible and appropriate remedies for the effective protection, reparation and restitution of the right to personal data protection, including compensation for damage caused by violations of the relevant laws and regulations;**

(b) **Acting in a sovereign capacity, identify and consider adopting aspects of other countries' data protection and privacy legislation that may offer stronger guarantees for the effective realization of these rights in the digital age;**

(c) **Promote and foster human rights information and education, particularly in the area of personal data protection and privacy, as a matter of priority, at all levels and in all fields, so that data subjects are aware of, understand and can exercise their rights and, if necessary, can avail themselves of remedies to ensure their effective enjoyment.**