



El futuro
es de todos

Consejería Presidencial
para asuntos económicos
y transformación digital



Sandbox on privacy by design and by default in Artificial Intelligence projects



SANDBOX ON PRIVACY BY DESIGN AND BY DEFAULT IN ARTIFICIAL INTELLIGENCE PROJECTS

The following document has been prepared by the **Superintendence of Industry and Commerce with inputs and technical guidance from the Presidential Council for Economic Affairs and Digital Transformation.** The realization of the sandbox and the conditions of its operation are the exclusive competence of the Superintendence of Industry and Commerce.

Date:

April, 2021

Entities involved in the preparation of the document





CONTENT

I

BACKGROUND

pág 4-5

II

SUMMARY OF THE MAIN ASPECTS
OF THE REGULATORY SANDBOX

pág 6-9

III

PRIVACY, ETHICS AND SECURITY
BY DESIGN AND BY DEFAULT

pág 10-12

IV

PRIVACY IMPACT ASSESSMENTS
(PIA)

pág 13-14

V

TRUST

pág 15-16

VI

REGULATORY FRAMEWORK

pág 17-19

VII

THE REGULATORY SANDBOX

pág 20-25

VIII

GLOSSARY

pág 26-28

IX

ACRONYM

pág 29-30



I

BACKGROUND



Privacy by design and by default is not incorporated in the Statutory Law 1581 of 2012. However, article 21 of said regulation states that the Superintendence of Industry and Commerce will exercise the following functions: “i) *Suggest or recommend adjustments corrections or an adequacy to the regulation that are consistent with technological, computer or communicational evolution; (...)*”.

On November 4, 2020, the first version for comments of the document “*Sandbox on privacy by design and by default in Artificial Intelligence projects*” was published on the website of the Superintendence of Industry and Commerce (SIC), in accordance observations were submitted. In this way, from the beginning, the participation of citizens and different actors of society was promoted.

As a result, seventeen (17) interventions and seventy-seven (77) comments were made by citizens; authorities; associations; organizations; and companies from various sectors. Such observations were answered by Document No. 002 of February 2, 2021.

Regulatory sandboxes are, among others, supervised spaces for temporary experimentation. There is no single concept of sandbox and, furthermore, not all of them operate the same or have the same aims nor approaches. National and foreign experiences on sandbox vary greatly in their essence, objectives and legal powers of the authorities in charge of them.

The Superintendence of Industry and Commerce carries out this sandbox on artificial intelligence (AI) because this initiative is not only consistent with the recommendations of CONPES 3975 of November 8, 2019 (National Policy for Digital Transformation and Artificial Intelligence), but because since March 18, 2019 the entity began to work on the processing of Personal Data in artificial intelligence.

Additionally, on the international scenario, the Superintendence of Industry and Commerce (SIC) has led and contributed to the drafting of documents on artificial intelligence, such as, for example, the one approved on June 21, 2019 by the Ibero-American Network for the Protection of Personal Data entitled “*General recommendations for the Processing of Personal Data in Artificial Intelligence*”.

Finally, the SIC has also participated in the drafting and promotion of the following document, approved in October 2020 by the GPA (Global Privacy Assembly): “*Adopted resolution on accountability in the development and use of artificial intelligence*”.



II

SUMMARY OF THE MAIN ASPECTS OF THE REGULATORY SANDBOX



This regulatory sandbox seeks to be a preventive and experimental space, so that companies interested in developing artificial intelligence projects create collaborative compliance solutions through the non-binding accompaniment of the Data Protection Authority. For instance, in the implementation of tools such as: privacy impact assessment (PIA); privacy by design and by default; accountability, among other measures that they consider appropriate.

The sandbox will be, among others, a space in order to accompany some artificial intelligence projects from the beginning with a view that they are not only scientifically or economically successful, but also friendly and respectful of the rights of people with regards to the collection, storage, use or circulation of their information.

It is relevant to emphasize that this project is carried out within the framework of the legal powers of the SIC, and that its development does not suspend any of the entity's legal duties. Therefore, it does not mean that the organizations or companies selected to be part of this sandbox are exempt from complying with the Personal Data Protection regulation during the execution of the artificial intelligence project, much less afterwards.

The essential characteristic of this sandbox project is that it is an advisory and guidance space in the structuring of the design of artificial intelligence projects that involve the processing of Personal Data.

The development of the regulatory sandbox on privacy by design and by default, is summarized in the following aspects:

SANDBOX ON PRIVACY FROM DESIGN AND BY DEFAULT IN ARTIFICIAL INTELLIGENCE PROJECTS	
Legal framework	Statutory Law 1581 of 2012 and Decrees 4886 of 2011 and 1377 of 2013 (incorporated in Decree 1074 of 2015).
Objectives	<ul style="list-style-type: none"> ○ Suggest or recommend, if necessary, adjustments, corrections or adaptations of Colombian regulations to the technological advances. ○ Establish criteria that facilitates compliance with the regulation on data processing and indicate the procedures for its full application. ○ Ensure that an adequate processing of personal data is an essential component of the design and implementation of artificial intelligence projects. ○ Promote the creation of artificial intelligence products that, from their design and during their execution, are, among others, respectful of people's rights regarding their personal information and in accordance with the regulations on the processing of personal data. ○ Accompany and advise on the protection of personal data, the selected companies, in order to mitigate the risks. associated with the implementation of artificial intelligence. ○ Consolidate a preventive / proactive approach to the protection of human rights in AI projects.
Main requirements	Artificial intelligence project in e-commerce, advertising or marketing that is in the design stage (it must not be completed or have been put into operation).
Who can participate?	<p>National and foreign companies, as well as public and private entities, whose initiatives meet, at least, the following requirements may participate:</p> <ul style="list-style-type: none"> ○ Artificial intelligence projects. ○ The project focus on e-commerce and/or advertising and marketing.

SANDBOX SOBRE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO EN PROYECTOS DE INTELIGENCIA ARTIFICIAL	
	<ul style="list-style-type: none">○ The project involves the processing of personal data.○ The project is in a design stage.○ The project has not started the processing of personal data.○ The project has not been completed or has been put into operation.
Selection	One, several projects or all projects can be selected. This depends, among others, on the impact and relevance in the processing of personal data.
Duration	Initial duration of one (1) year.
Expenses	The presentation of proposals has no cost.
Tools	Specialized advice from the SIC on legal aspects regarding the processing of personal data and monitoring the progress of the project.





III

PRIVACY, ETHICS AND SECURITY BY DESIGN AND BY DEFAULT



The Global Privacy Assembly approved in October 2020 the **RESOLUTION ON ACCOUNTABILITY IN THE DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE**. The resolution, among others, urges organizations that develop or use artificial intelligence (AI) systems to consider implementing the following measures:

- **Assess** the potential impact to human rights (including data protection and privacy rights) before the development and/or use of AI.
- **Test** the robustness, reliability, accuracy and data security of AI before putting it into use, including identifying and addressing bias in the systems and the data they use that may lead to unfair outcomes.
- **Implement** accountability measures that are appropriate with respect to the risks of interference with human rights.

During 2019 the Superintendence of Industry and Commerce (SIC) published the following documents: (i) **Guidelines for the processing of personal data for e-commerce purposes**¹; (ii) **Guidelines for the processing of personal data for marketing and advertising purposes**²; (iii) **Guidelines for the implementation of the Principle of Accountability in international transfers of personal data**³. In all of them, it is recommended to incorporate privacy, ethics and security by design and by default. Additionally, it is suggested to make Privacy Impact Assessments (PIAs).

The aforementioned guidelines are applicable to any activity like, among others, artificial intelligence (AI). In fact, the guidelines are reiterated in the **“General Recommendations for the Processing of Personal Data in Artificial Intelligence”**⁴ of the Ibero American Data Protection Network (RIPD by its acronym in Spanish).

In those documents it is suggested that privacy by design and by default is considered as a proactive measure to, among others, comply with the Principle of Accountability. By introducing the principle of privacy by design and by default, it seeks to guarantee the adequate processing of the data that is used in the projects that involve the collection, use or processing of personal data. So, an adequate processing of the information must be an essential component of the design and implementation of AI projects.

Privacy by Design **“advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization’s default mode of operation”**⁵. Consequently, even before collecting information

and during its whole lifecycle, preventive measures of diverse nature (technological, organizational, human, and procedural) shall be adopted. Through this, organizations can avoid violating the right to privacy and confidentiality of the information of the data subjects.

Ethics by design and by default, must irradiate the whole scheme, development, and use of products or AI processes; thus, being part of the DNA of any AI project.

The aforementioned must also be said about security by design and by default when processing data in AI. Without safeguards there is no privacy in the rightful processing of personal data. It is of special importance to adopt technological, human, administrative, physical and contractual measures in order to fulfill the following objectives:

- **Avoid the wrongful or unauthorized access to data.**
- **Avoid the manipulation of data.**
- **Avoid the destruction of information.**
- **Avoid the wrongful or unauthorized uses of data.**
- **Avoid circulation of data to unauthorized people.**

Safety measure must be appropriate and must take into consideration various factors, such as the following: (i) the levels of risk in the processing; (ii) the nature of the data; (iii) the magnitude of the harm that can be caused to the data subjects and the Controller if the data is wrongly processed; (v) the size of the organization; (vi) the available resources; (vii) the monitoring of the reliability of algorithms; (viii) the state of the art; (ix) the context and purpose of the processing of data; (x) the cross-border circulation of data; and (xi) the uncertainty and complexity of each AI initiative.

Said measures must be object of revision, evaluation, and permanent improvement.





IV

PRIVACY IMPACT ASSESSMENTS (PIA)



Prior to the design and development of the AI project, the SIC and the RIPD suggest conducting a privacy impact assessment (PIA). In order to put into operation an effective system of risk management and internal controls, to guarantee that the data is processed properly and in accordance with the existing regulation.

Such an evaluation should include, at a minimum, the following:

- A detailed description of the operations that involve the processing of personal data in the development of AI.
- A risk assessment, specifically with regards to the rights and liberties of the data subject. It is essential that organizations develop and implement, among others, a ***"risk management system associated with the processing of personal data"*** that allows them to ***"identify, measure, control and monitor all those events or situations that may affect the proper management of the risk to which they are exposed in development of the fulfillment of the norms of protection of personal data"***.
- Measures implemented to mitigate risks, including guarantees, security measures, software design, technology and mechanisms. All the measures must be implemented taking into account the rights and interests of the data subjects as well as third parties that may be affected by this.

The results of the PIA, along with the measures taken to mitigate risks shall be implemented as part of the privacy by design and by default.





V TRUST



For some decades it has been argued that trust is a crucial factor for the growth and consolidation of any other activity carried out through the use of technologies, which has been reiterated by stating that "***continuous trust-building activities must be one of the most important strategic priorities for each organization***".

Trust is understood as the expectation that "***the other's word can be counted on***" and that positive and beneficial actions will be taken between the parties in a reciprocal manner. When there is trust, the person believes that the company is trustworthy, keeps its word, is sincere, with integrity and fulfills the promised actions.

Trust, as a key element in digital environments, arises "*due to the need for responsible processing of information (...) and that consumers 'feel' that technology is responding to their security and privacy requirements (...)*".

Implementing privacy by design and by default is evidence that organizations are committed to the adequate processing of personal data and the rights of data subjects. Therefore, participating in this sandbox is a mechanism that, among others, can generate trust in the market and, in general, in the public, since the participating organizations demonstrate that they have taken into account, since the design of the AI project and with the support of this Superintendence, the regulation of personal data protection.





VI

REGULATORY FRAMEWORK



The regulatory sandbox is carried out within the framework of the following legal powers of the Superintendence of Industry and Commerce:

Decree 4886 of 2011 "*Through which the structure of the Superintendence of Industry and Commerce is modified, the functions of its dependencies are determined, and other provisions are issued*".

Article 1. GENERAL FUNCTIONS

"The Superintendence of industry and commerce will exercise the following functions:

*1. Advise the National Government and participate in the formulation of policies in all matters that have to do with consumer protection, the promotion and protection of competition, industrial property, **the protection of personal data** and other areas of its knowledge.*

(...)

*61. Provide instructions on consumer protection, competition protection, industrial property, **administration of personal data** and in the other areas of their functions, **set criteria that facilitate compliance and indicate the procedures** for their full application.*

(...)

*65. Carry out activities of dissemination, **promotion** and training, in matters of competence of the entity (...)"*.

Article 3. FUNCTIONS OF THE OFFICE OF THE SUPERINTENDENT OF INDUSTRY AND COMMERCE.

The functions of the Office of the Superintendent of Industry and Commerce are:

*1. Advise the National Government and participate in the formulation of policies in all those matters that have to do with consumer protection, the promotion and protection of competition, industrial property, **the protection of personal data** and in other areas of its function.*

(...)

*5. Provide instructions on consumer protection, competition protection, industrial property, **the protection of personal data** and in the other areas of their functions, as well as setting **criteria that facilitate compliance and indicating the procedures** for their full application.*

Article 16. FUNCTIONS OF THE OFFICE OF THE DELEGATED SUPERINTENDENT FOR THE PROTECTION OF PERSONAL DATA.

The functions of the Office of the Deputy Superintendent for the Protection of Personal Data are:

- 1. Advise the Superintendent of Industry and Commerce in the formulation of policies in relation to its area.*
- 2. Ensure **compliance** with current laws and regulations and propose new provisions. (...) "*

- Statutory Law 1581 of 2012 "By which general provisions for the protection of personal data are issued".**

Article 21. FUNCTIONS

"The Superintendence of Industry and Commerce will exercise the following functions:

(...)

- i) Suggest or recommend adjustments, corrections or adaptations to the regulations that are consistent with technological, computer or communicational evolution; (...)"*





VII

THE REGULATORY SANDBOX



The regulatory sandbox on privacy by design and by default aims national and foreign companies as well as public and private entities that are interested in developing AI projects, so that, in a preventive and experimental space, and from the design stage of the initiatives, collaborative compliance solutions to the regulation of personal data protection are created, through the non-binding accompaniment of the data protection authority.

The foregoing with the intention of implementing in said projects various tools such as privacy impact assessments, privacy by design and accountability, among other measures that they consider appropriate.

The SIC proposes this regulatory sandbox to be a space to accompany some artificial intelligence projects from the beginning with a view to ensuring that they are not only scientifically or economically successful, but also friendly and respectful of people's rights regarding collection, storage, use or circulation of their information.

The projects that are postulated in this sandbox will focus exclusively on the design phase of the AI project.

During the development of the sandbox, an exercise of collaborative creation of solutions in terms of data protection and artificial intelligence is activated. This sandbox will be positive for entrepreneurs and their clients because technological innovation will be accompanied by specialized advice in order for it to be compatible with the protection of personal data so that their products are, among others, respectful of people's rights regarding collection and use of their information.

Sandbox transversality and participation of other public and private entities

The SIC considers that the knowledge and elements obtained from this experimentation space can be very positive for other public and/or private entities. In general terms, it has been determined that the characteristics of artificial intelligence and its impact on different regulations cause different organizations to be involved in an exercise of these characteristics.

The entities involved can obtain adequate knowledge about tools to develop privacy by design in the transformational projects they are developing and the use of AI systems in their entity. Likewise, information asymmetries on technology are reduced to make informed regulatory decisions and it is possible to know the posture of the SIC on the matter, to avoid possible contradictions with other supervisory or regulatory entities.

The above has already been pointed out in different technical documents on the subject, such as the **Conceptual Model for the design of Regulatory Sandboxes & Beaches in AI** proposed by Armando Guío and published by the Presidential Advisor for Economic Affairs and Digital Transformation in 2020:

“Therefore, considering that a technology with these characteristics can be analyzed from a single discipline or from a single surveillance and control authority can be quite limited. Technologies this disruptive have cross-cutting effects and require different professionals and authorities to provide a multidisciplinary approach. Now, it is enough to just imagine the ambitious effects of a single transversal sandbox that provides lessons and teachings to different sectors and entities within the State. Not only are the benefits seen in terms of efficiency for the public sector, but it also serves as a basis for considering the future construction of a transversal regulation of emerging technologies such as artificial intelligence, which avoids a sectorized approach that may even become contradictory”⁹.

Consequently, the regulatory sandbox model proposed will present a specific mechanism for the participation of other public and/or private entities as active participants and observers of the work carried out in this regard.

The SIC will invite organizations to participate depending on their corporate purpose or legal competences so that they are pertinent or related to the project that is selected to carry out the sandbox.

Specific objectives

- Establish criteria that facilitate compliance with the regulation on data processing and indicate the procedures for its full application.
- Suggest or recommend, if necessary, adjustments, corrections or adaptations of the Colombian regulation to technological advances.
- Ensure that adequate processing of personal data is an essential component of the design and implementation of artificial intelligence projects.

- Promote the creation of artificial intelligence products that, from their design and during their implementation, are, among others, respectful of people's rights regarding their personal information and in accordance with the regulation on the processing of personal data.
- Accompany and advise on the protection of personal data to the selected companies, in order to mitigate the risks associated with the implementation of artificial intelligence.
- Consolidate a preventive/proactive approach to the protection of human rights in AI projects.

Benefits

For the country:

- Promote respectful innovation standards on the processing of personal data of its citizens.
- Lead the generation of AI projects that are references for future ventures.

For participating companies:

- Decrease of legal risks in the processing of personal data.
- Specialized support from the authority in the development of tools for data protection by design and by default.
- Generate trust in the market, its customers and society.
- The SIC will analyze and determine if the participants comply with standards of accountability in the event of investigations and imposition of sanctions. The principles of the Colombian data protection regulations and their application in the design and implementation of artificial intelligence technologies will be evaluated.

For citizens:

- Be users of AI products respectful of their rights as a data subject or, as the case may be, know that their data is being collected and used by companies that have implemented privacy by design and by default.
- More trust because they know that the data protection authority was involved in the project.

For the SIC:

- The sandboxes are a preventive alternative to comply with the mandate of article 15 of the Constitution according to which: "*in the collection, processing and circulation of data, freedom and other guarantees enshrined in the Constitution will be respected*".

- Promote data processing that is respectful of human rights.
- Understand and know first-hand the innovations of the companies that are subject of control and surveillance.
- Evaluate "in real time" the effectiveness of the entity's strategies for the protection of rights.
- Consolidate knowledge of the SIC regarding personal data by creating instruments that can be used by other companies, even if they have not participated in the sandbox.

Requirements

National and foreign companies may participate, as well as public and private entities.

The projects that participate in the call must meet the following requirements:

- Artificial intelligence projects.
- The project focus on e-commerce and/or advertising and marketing.
- The project involves the Processing of Personal Data.
- The project is in a design stage.
- The project has not started the Processing of Personal Data.
- That the project has not been completed or has been put into operation.

Queries and doubts

Any questions may be sent to the following email address: **megutierrez@sic.gov.co**.

If necessary, some work sessions may be convened with all interested parties. Timely notice of these sessions will be given, along with the details of the location (virtual or in person), date and time of completion.

Presentation of proposals

Those who wish to submit their proposals must fill out the form that will be available at the sandbox website, within the time limit set for it.

The SIC may request additional information if necessary.

Selection

The SIC may select one or more of the proposals.

The results will be published on the dates announced at the sandbox website, which may be modified if necessary.

The SIC may not select any of the proposals submitted.

Project development

The project will begin in July 2021 and the SIC's advice will be for a minimum of one (1) year. However, if necessary, said term may be extended by an equal, lower or higher term, depending on the case.

Prior to initiating operations of the sandbox, meetings will be held with the selected company/ companies and the SIC to establish specific aspects of the sandbox execution such as, among others, the work schedule, the delimitation of the expectations and responsibilities of the parties.

Said agreements will be in writing as evidence of the commitments of the parties and traceability of the advice of this entity within the sandbox.

During the development, the office of the Deputy Superintendent for the Protection of Personal Data will carry out the corresponding controls, which include, but are not limited to, reports with feedback, recommendations and observations.





VIII

GLOSSARY





- + **Consent:** “Prior, express and informed consent of the data subject to carry out the Processing of Personal Data”.¹¹

- + **Database:** “Organized set of personal data that is subject to Processing”.¹²

- + **E-commerce:** All those *“issues raised by any relationship of a commercial nature, whether contractual or not, structured from the use of one or more data messages or any other similar means (...)”*.¹³

- + **Personal data:** “Any information linked or that may be associated with one or more specific or determinable natural persons”.¹⁴

- + **Processor:** *“Natural or legal person, public or private, that by itself or in association with others, carries out the Processing of Personal Data on behalf of the Controller of the Processing”*.¹⁵

- + **Artificial Intelligence:** *“Field of computing dedicated to solving cognitive problems commonly associated with human intelligence or intelligent beings, understood as those that can adapt to changing situations. Its basis is the development of computer systems, the availability of data and algorithms”*.¹⁶

- + **Marketing:** *“The result of the activity of the companies that directs the flow of goods and services from the producer to the consumer or user, with the aim of satisfying consumers and allowing them to achieve the objectives of the companies”*.¹⁷

- + **Privacy by design (PbD):** Approach to be applied by the Data Controller oriented to the risk management and proactive responsibility to establish strategies that incorporate the protection of privacy from the design in determining the means of processing personal data, during it and before collecting personal data. In particular, with the incorporation of preventive measures of various kinds that allow the principles, rights and other obligations set forth in the personal data protection regulations to be applied effectively.¹⁸



- + **Privacy by default (PDpD):** Proportional processing that the Data Controller must make of the personal data with respect to the purpose for which they were collected, in such a way that, its programs, services, computer systems or platforms, electronic applications or any other technology that imply a processing of personal data, incorporate minimally intrusive processing alternatives.¹⁹

- + **Advertising:** Any form and content of communication that is intended to influence consumer decisions.

- + **Regulatory sandbox:** Preventive space, temporary and supervised experimentation so that national and foreign companies, and public or private entities interested in developing artificial intelligence (AI) projects, from the design stage of these initiatives, create solutions for collaborative compliance with the regulations of personal data protection.²⁰

- + **Controller:** *“Natural or legal person, public or private, that by itself or in association with others, decides on the database and / or the Processing of the data”.*²¹

- + **Data subject:** *“Natural person whose personal data are subject to Processing”.*²²

- + **Processing:** *“Any operation or set of operations on personal data, such as the collection, storage, use, circulation or deletion”.*²³



IX

ACRONYM





- + **AI:** Artificial Intelligence
- + **RIPD:** Ibero American Data Protection Network
- + **PbD:** Privacy by design
- + **PDpD:** Privacy by default
- + **PIA:** Privacy Impact Assessment



References

- 1 Official document (Spanish version): [https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf)
- 2 Official document (Spanish version): <https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf>
- 3 Official document (Spanish version): [https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales%20\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales%20(1).pdf)
- 4 Official document: [https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20\(2019\)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20(2019)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE(1).pdf)
- 5 Cavoukia, Ann. Privacy by design the 7 foundational principles
Available in: <http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf>
- 6 Edelman Trust Barometer of 2019, <https://www.edelman.com/trust-barometer>
- 7 Cfr. Barrera Duque, Ernesto (2018) *Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales*. Universidad de la Sabana y Ecoe ediciones.
- 8 Cano M, Jeimy J. (2019) Confianza digital imperfecta: *Un reto de simetría, reciprocidad y sinceridad*. Available at: <https://www.linkedin.com/pulse/confianza-digital-imperfecta-un-reto-de-simetría-y-cano-ph-d-cfe/>. European Commission, Brussels, 19.2.2020. COM (2020) 65 final. White Paper on Intelligence - a European approach to excellence and trust.
- 9 Guío Español, Armando. Modelo conceptual para el diseño de Regulatory Sandboxes & Beaches en IA. Corporación Andina de Fomento y la Consejería Presidencial de Auntos Económicos y Transformación Digital, 2020. Pg. 10. Available at: <https://dapre.presidencia.gov.co/AtencionCiudadana/DocumentosConsulta/consulta-200820-MODELO-CONCEPTUAL-DISENO-REGULATORY-SANBOXES-BEACHES-IA.pdf>
- 10 En efecto, el último párrafo del artículo 27 del decreto 1377 de 2013 (incorporado en el decreto 1074 de 2015) dice lo siguiente: “*La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tomada en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto.*”



References

- 11 Literal a) of Article 3 of Statutory Law 1581, 2012
- 12 Literal b) of Article 3 of Statutory Law 1581, 2012
- 13 Literal b) of Article 2 of Law 527, 1999.
- 14 Literal c) of Article 3 of Statutory Law 1581, 2012
- 15 Literal d) of Article 3 of Statutory Law 1581, 2012
- 16 CONPES Document 3975 of 2019. Pg. 20. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/3975.pdf>
- 17 McCarthy, E.J. (1964): Basic Marketing: A Managerial Approach, 2a ed., R.D. Irwin, Homewood.
- 18 Ibero-American Data Protection Network (RIDP) (2017). Personal Data Protection Standards for Ibero-American States. Available at: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf and Agencia Española de Protección de Datos (2019) Guía de Privacidad desde el Diseño. Disponible en: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf>
- 19 Ibero-American Data Protection Network (RIDP) (2017). Personal Data Protection Standards for Ibero-American States. Available at: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Agencia Española de Protección de Datos (2020) Guía de Protección de Datos por Defecto. Available at: <https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf>
- 20 Cf. Inter-American Development Bank (2018). Regulatory Sandbox in Latin America and the Caribbean for the FinTech ecosystem and the financial system. Available at: <https://publications.iadb.org/publications/spanish/document/Sandbox-regulatorio-en-América-Latina--el-Caribe-para-el-ecosistema-Fintech-y-el-sistema-financiero.pdf>. Cf. Information Commissioners's Office -ICO- *What is the Sandbox?* Available at: <https://ico.org.uk/sandbox>
- 21 Literal e) del artículo 3 de la Ley 1581 de 2012
- 22 Literal f) del artículo 3 de la Ley 1581 de 2012
- 23 Literal g) del artículo 3 de la Ley 1581 de 2012



El futuro
es de todos

Consejería Presidencial
para asuntos económicos
y transformación digital



Sandbox on privacy by design and by default in Artificial Intelligence projects

