GALA
GLOBAL ADVERTISING LAWYERS ALLIANCE

Privacy Law: A Global Legal Perspective
on Data Protection Relating to Advertising and Marketing

Published in Cooperation with the IAA
INTERNATIONAL ADVERTISING ASSOCIATION

Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing

FOREWORD

Advertising has changed dramatically over the past decade. Rapid developments in technology, the proliferation of social media, and increased access to consumer data have allowed publishers, brands, agencies, and other players in the advertising ecosystem to better understand consumers and deliver more relevant content. Consumer data is incredibly valuable and can be used for purposes such as research and analysis, calculating attribution for campaigns, email and text marketing, delivering personalized advertising, and finding prospective customers in ways not previously possible. For example, a brand can upload its customer list to a social media platform, and serve advertising on the platform to both customers on that list as well as segments of customers identified by the platform as similar to the brand's customers and likely to purchase the brand's products.

The increased reliance on consumer data has led to inevitable questions about the need for regulation over consumer privacy. While privacy is not a new concept, privacy exploded on a global scale in 2018 due to a combination of factors. Most significantly, the European Union began enforcing its robust data protection law, the General Data Protection Regulation (GDPR), which gave regulators the ability to issue dramatic penalties against companies for improperly processing data about individuals located in Europe. Concerned about the ease of data flows across borders and the growing importance of international markets, companies around the world took measures to address the obligations of the GPDR. At the same time, the world learned about the Facebook-Cambridge Analytica incident, which created heightened awareness of the power of data and the potential for misuse.

Privacy compliance has shifted from a business best practice to a business necessity. Since 2018, numerous jurisdictions have updated their privacy laws to bring them closer to GDPR standards. For instance, California and Brazil both passed GDPR-like privacy laws, effective in 2020. While many of the new laws share similarities to the GDPR, they differ in key aspects and require independent analysis. Companies must now understand the

nuances between privacy obligations in their home jurisdictions and those elsewhere, and implement procedures and systems to harmonize compliance.

This book, developed by the Global Advertising Alliance (GALA), in cooperation with the International Advertising Association (IAA), is the first, to our knowledge, designed specifically to address global privacy laws in the context of the advertising ecosystem. GALA members across 70 countries with expertise in privacy in their respective jurisdictions helped develop the content for the book. Each chapter covers a specific country, giving a background on the privacy framework for that country, detailing key issues in relation to advertising, and concluding with opinions from the author of that chapter as to the state of privacy in that country. To improve readability of the book, GALA divided the book into two parts. Part one focuses on countries outside the European Union, while part two starts with an overview of the GDPR and then focuses on countries within the European Union that are subject to the GDPR. The digital version of the book includes both parts.

While there are great differences in the ways that privacy is addressed around the world, there are certainly some key trends across jurisdictions:

- Countries are more focused than ever before on privacy, and many are developing robust laws with harsh penalties. However, compliance can be difficult because laws often are not technologically agnostic and struggle to fit advancements in technology.

- The types of consumer data considered to be personally identifiable have broadened substantially. Information previously treated by the advertising ecosystem as "de-identified" or "anonymous," such as IP addresses and Ad IDs, could fall within scope of privacy laws.

- Transparency and choice are becoming universal concepts. Privacy laws around the world accept the notion that consumers have the right to know what information is being collected from them and the purposes for which it is being collected. They also frequently give consumers the right to limit use of their information for marketing purposes. Depending on the jurisdiction and other factors, choice may require opt-in or opt-out consent.

- Practices that are not specifically prohibited by law could still violate the law or create public relations issues if those practices do not meet the reasonable expectations of consumers. Providing better notice to consumers and avoiding "creepy" practices can help address potential issues.

- In response to globalization, some countries have instituted strict data localization requirements. Cross-border data flows require additional consideration.

- Global data security and breach response obligations have dramatically evolved over the past decade, playing catch up to those already found under U.S. law. Violations often carry harsh penalties.

- Privacy regulation comes not just from lawmakers, but also from the platforms and browsers from which data is collected. Changes to their policies and technology have a fundamental impact on the advertising ecosystem and privacy compliance efforts.

- Profiling and automated decision-making carry increased scrutiny. Many jurisdictions impose specific obligations, such as internal assessments, around related data processing.

- Jurisdictions do not always align on balancing privacy, surveillance, and freedom of speech. Companies should aim to understand local belief systems and practices when processing data about consumers related to that jurisdiction.

It is important to note that this book reflects a snapshot in time and was developed prior to the COVID-19 pandemic of 2020. As such, the content does not address the impact of COVID-19 on privacy law. Countries around the world have taken measures to combat COVID-19, including through development of apps designed to trace the spread of COVID-19 that rely on the processing of vast amounts of consumer data. These measures may have a short term impact on privacy rights and expectations, and could ultimately result in long term increased privacy regulation as consumers become more concerned

about how their data is used. We reserve discussion of the impact of COVID-19 for the next edition of this book.

A big thank you to all of the GALA members who contributed to this book, and, in particular, to Soren Pietzcker (who also led the writing of the GDPR chapter) and to Lyric Kaplan (who helped develop the questions for the book), as well as to the IAA for its collaboration efforts. This book would not be possible without all their hard work. Special thank you to Stacy Bess (Executive Director of GALA), Jeff Greenbaum (Chairman of GALA), Srinivasan Swamy (Chairman & World President of IAA), Carla Michelotti (Global VP of Government Affairs of IAA), and Dagmara Szulce (Managing Director of IAA).

On behalf of GALA, we appreciate you choosing to read our book, and hope you find it to be a valuable resource.

Daniel Goldberg
Frankfurt Kurnit Klein & Selz, PC

May 15, 2020

INTRODUCTION

For over eight decades, the International Advertising Association (IAA) has played a significant role globally identifying and educating marketing and advertising thought leadership about key industry issues by promoting and defending freedom of commercial speech; establishing and supporting effective and meaningful advertising industry self-regulation; defending the value of brands, and their important role in consumer choice; and in the digital world encouraging respect for consumer privacy while promoting the growth of digital commerce and communication.

In April 2019, some of IAA Board members called on Jeffrey A. Greenbaum, Chairman of the Global Advertising Lawyers Alliance (GALA) and also the Managing Partner of Frankfurt Kurnit Klein & Selz PC in his New York office to discuss privacy and the current digital environment.

In the course of the discussions, we talked about the digital privacy issues that are raging in different parts of the world and how governments are coming up with a wide variety of laws to protect their people. We also talked about how difficult it was for businesses to navigate the landscape of different, and ever-changing, rules – and that they needed additional resources they could turn to, for reference. Jeff promptly agreed that through its extensive network of lawyers in various countries, GALA is well equipped to put together a handbook on the multiplicity of privacy laws that impacts advertising and marketing. This, we felt, would be a much-needed compendium. It would be an important resource for large companies who are operating in different geographies to turn to, with communication seamlessly flowing across borders.

Over the last several months, GALA's members from around the world have distilled the details of the privacy laws impacting advertising and marketing in more than 70 countries, providing critical information about the laws and regulations that protect persons consuming digital media and those who are targeted by digital marketing.

We hope that this Global Privacy Laws handbook will be an excellent reference volume to all major marketing companies and governments around the world. The book demonstrates how some countries have simple laws that are easy to follow and how some countries have made the laws quite complex.

IAA invited GALA to become an institutional member and take on a Board position at IAA. The association between the two global institutions could gain from each other, as both serve the interest of Marcom practitioners. IAA believes that its promise of being Global Compass for Marketing Communications is consistent with GALA's view.

We do know that this professional labor of love by GALA lawyers is a welcome addition to many law books that are available in the world. IAA is indeed delighted to have been associated in bringing out this landmark book for the benefit of the industry.

We thank the GALA team for the enormous effort and thought leadership that went into creating this valuable global resource.

Srinivasan K. Swamy
IAA Chairman & World President

June 3, 2020

ABOUT GALA

The Global Advertising Lawyers Alliance (GALA) is the leading network of advertising lawyers in the world. With firms representing more than 90 countries, each member has the local expertise and experience in advertising, marketing and promotion law that will help your campaign achieve its objectives, and navigate the legal minefield successfully. GALA is a uniquely sensitive global resource whose members maintain frequent contact with each other to maximize the effectiveness of their collaborative efforts for their shared clients. GALA provides the premier worldwide resource to advertisers and agencies seeking solutions to problems involving the complex legal issues affecting today's marketplace.

For further information about GALA, please contact the relevant member directly or alternatively GALA's Executive Director, Stacy Bess at:

Global Advertising Lawyers Alliance
28 Liberty Street, 35th Floor, New York, NY 10005
Tel: 212.705.4895 | Fax: 347.438.2185
Email: sbess@galalaw.com
www.galalaw.com

TABLE OF CONTENTS

ECUADOR

1 PRIVACY LAW

1.1 How is privacy regulated in Ecuador?

Ecuador does not have a Data Protection Law; however, the Constitution recognizes and guarantees the protection of personal data, establishing that the authorization of the data owner is necessary for any collection, filing or dissemination.

In addition to the constitutional regulations, there are regulations scattered in various legal instruments that refer to the protection of personal data for specific issues, with some inconsistencies and without procedural rules, such as the Organic Telecommunications Law, the Monetary and Financial Organic Code and the Public Data Registration Law.

Therefore, the absence of specific technical regulation on the matter and the lack of an expedited course of action to enforce rights, have left data privacy behind in Ecuador with almost an un existing actual protection to the data owner.

However, a specific Bill for the protection of personal data was presented by the Executive Branch to the National Assembly on September 19, 2019 which will regulate in detail this matter in a very similar way to the GDPR in Europe. This Bill may take several months more to be approved.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The laws that regulate data protection in Ecuador and are relevant here are the following:

(a) Constitution of the Republic of Ecuador, Articles 66(11), (19), (20) and 92: Article 66 recognizes and guarantees data protection. Article 92 determines that the authorization of the owner of the data is necessary, both in order for data to be collected and to be disseminated.

Problem: The Constitution of Ecuador recognizes the protection of personal data, without giving a specific definition, which leaves it open to interpretation as to ownership of the right. In addition, no competent authority is established to regulate or supervise compliance with the few existing rules on protection within the Ecuadorian legal system. This is left to a *habeas data* proceeding before a regular judge, which is not usually effective.

(b) Organic Law of Jurisdictional Guarantees and Social Control, Articles 49 and 51: In accordance with the Constitution, these contemplates the *habeas data* proceeding.

(c) Organic Law of Telecommunications, Articles 22, 24, 78, 80, 81 and 82: These Articles set out rules on the rights of customers using telecommunication services, the obligations of telecommunication service providers, the right to privacy and the commercial use of personal data.

(d) Organic Monetary and Financial Code, Articles 352–360: These develop some scarce regulation on the protection of personal information of users of the national financial system, which is managed by the financial institutions in Ecuador.

(e) Regulations for the Management of Confidential Information in the National Health System, Articles 17, 27 and 38: These contain some regulation on the matter; however, they confuse “confidential information” and “sensitive data”.

(f) Labour Code, Article 42(7): This imposes an obligation on employers to have and update their workers' data.

(g) Organic Code of the Social Economy of Knowledge, Creativity, and Innovation, Articles 140 and 141, General Provisions 26 and 27: These address personal data from an intellectual property point of view, stating that personal data is not part of the protectable matter of databases.

(h) Public Data Registration Law: This is not a personal data law, as it doesn't interfere with private databases. It does not define personal data and is limited to regulating the compilation of information contained in the different public offices.

(i) Comprehensive Organic Criminal Code, Articles 178 and 229: This typifies punishable activities regarding illegal database disclosure and violation of privacy, however, it confuses "confidential information" and "intimacy rights".

(j) Pronouncements of the Constitutional Court of Ecuador:

(i) Sentence No. 001-14-PJO;

(ii) Sentence No. 002-11-SIN-CC.

(k) Bill for Personal Data Protection: This was presented to the Assembly in September 2019; it clarifies the subject and all its concepts, becoming a comprehensive regulation with international standards.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

Since Ecuador does not have a law for the protection of personal data, and the scattered regulations do not contemplate any specific proceedings, it is necessary to follow the provisions of the Constitution, which, through a *habeas data* proceeding, guarantee access to personal data, through which the owner of such information may request for it to be rectified, deleted or updated, or simply seek access to it.

The Organic Law of Jurisdictional Guarantees and Constitutional Control states that *habeas data* actions must be filed before the competent judge where the transgression takes place. Although it is not a complex proceeding, it is not simply an execution or compliance process, and may require a public hearing and the presentation of evidence.

The Bill for Personal Data Protection simplifies the situation and establishes a specific proceeding for this, which is handled through an administrative procedure before the Personal Data Protection Authority (which has yet to be created).

2 SCOPE

2.1 Which companies are subject to privacy law in Ecuador?

According to the Constitution, any entity, public or private, that handles information or personal data of any person, is subject to privacy rules.

2.2 Does privacy law in Ecuador apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Currently, in Ecuador, there is no specific rule about the scope of application of privacy laws; however, the Bill for Personal Data Protection will establish that it is applicable even when data processors are not domiciled in Ecuador, but the data owners are.

In addition, the Bill provides rules regarding data transfer to other countries (international transfer) in both the public and private sectors. Companies or economic groups must have binding corporate policies and regulations regarding data protection, which must be approved by the Authority.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Ecuador?

Although, Ecuador has various piecemeal rules on data protection, it does not have a specific rule that clearly defines what "personal data" really means and often confuses it with "confidential information" and "intimacy rights".

The Bill for Personal Data Protection, however, defines "personal data" as "data that identifies or makes identifiable a natural person, directly or indirectly, in the present or future". This definition includes metadata and data fragments.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" in Ecuador is treated in general by the Constitution as personal data that reveals racial, ethnic or religious origin, political positions, trade union membership, and data concerning health, sexual life or any other personal data that may cause discrimination in the life of the owner. There are no specific obligations regarding sensitive information.

The Bill defines "sensitive data" as data "related to ethnicity, gender identity, cultural identity, religion, political affiliation, judicial past, immigration status, sexual orientation, health, biometric data, genetic data and those whose improper processing may give rise to discrimination". In addition, the Bill opens up the possibility that the Personal Data Protection Authority may implement other categories of sensitive data.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

The primary source of the principles governing data privacy are set out in Article 92 of the Constitution of Ecuador, which contains various rights for data owners, which companies must respect in the processing of information.

Transparency: All persons have the constitutional right to know about the existence of any data about them that is being held in both public and private companies, as well as its usage. This principle is based on the consent of the owner. One example of the transparency principle is in Article 79 of the Telecommunications Law, which establishes that, in the event of a particular risk of a breach of the security of the public network or the telecommunications service, subscribers must be informed and the necessary measures must be taken to avoid the damage.

Purpose limitation: For example, Article 82 of the Telecommunications Law determines that companies that provide telecommunications services may not use personal data of customers without prior express consent, which should specify what data and information may be used and for how long and for what purpose.

Security: Article 74 of Telecommunications Law establishes a series of technical security and invulnerability measures that companies must follow for the use of personal data and information. The main objective of this is to preserve the right to privacy mentioned in the Constitution. Similarly, Article 80 establishes the obligation on telecommunication companies to implement internal procedures to deal with requests for access to personal data and the supervision and control thereof, following the provisions of the Agency for Regulation and Control of Telecommunications.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

As mentioned before, at this time there is no Privacy Law that specifically regulates the roles of companies with respect to personal information/personal data.

However, in the Bill currently being discussed by the Assembly, roles are established for both, those in charge and those responsible for the processing and protection of personal data affecting their obligations, for instance:

(a) **Obligations of data controllers**: Article 71 of the Bill establishes a series of obligations that the data controller will have to comply with, ranging from technical requirements to the need to sign confidentiality contracts and permanent updating and registration.

(b) **Obligations of Obligations of data processors**: Article 72 of the Bill contains the roles of the data processor, which relate mainly to the security measures to be implemented.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

At present, there is no Privacy Law that specifically regulates the key obligations with a focus on advertising, but, throughout the Bill, obligations are imposed on the handling of data, specifying that use is limited by the consent of the owners. Without the consent of the data owner, information cannot be treated, used or transferred.

Under the Bill, the obligations imposed on the controllers and processors include, amongst others, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, and registering with a privacy authority.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Ecuador? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

As stated above, data security regulations are dispersed within the Ecuadorian legal system.

Some of the standards that contain minimum regulatory parameters are:

(a) Paragraph 19 of Article 66 of the Constitution (in force since 2008) stipulates the right to the protection of personal data. However, it is not yet regulated, as in two other countries in the region: Venezuela and Bolivia.

(b) Article 229 of the Comprehensive Organic Criminal Code punishes with one to three years of prison anyone who discloses data that "violates the secrecy, intimacy, and privacy of individuals". If the person is a public servant or bank employee, the penalty is three to five years.

(c) Article 360 of the Organic Monetary and Financial Code prohibits the commercialization of credit references. The Superintendence of Banks has until September to assume the management of these records.

6.2 How are data breaches regulated in Ecuador? What are the requirements for responding to data breaches?

Currently, in Ecuador, there is no clear and specific procedure for responding to security breaches. In principle, an investigation of the facts is initiated by the Attorney General's Office and, subsequently, the possible actions to be presented are analyzed following the criminal proceedings and regulations established at the time.

On September 16, 2019, Ecuador was the victim of a massive exposure of private data of more than 20 million of its citizens by a company called Novaestrat, which led to questioning and evaluating the actions being taken to protect this type of information.

In the case of Novaestrat, the damage was caused by a security incident due to a bad configuration of a database. It is important that companies not only dedicate time and resources to the technological aspects of security, such as encryption solutions or prevention of information leaks, but also to the development of processes and security policies that include appropriate controls and contribute to the proper management of security.

This case was the catalyst for the Bill for Personal Data Protection to be sent to the Assembly for approval.

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The Ecuadorian legal system, specifically the Constitution, states that persons have the right to know of the existence of and have access to their data held by public and private entities. Also, it grants citizens the right to know the use, purpose, origin, and destination of their information, plus the duration of the file or data bank, the rectification of data and the requirement of authorization of any data transfer. Personal data protection is a Constitutional right; and so use of personal data must respect the owners' honor and full enjoyment of their rights.

The Telecommunications Law determines that providers of telecommunications services must adopt appropriate technical and management measures to preserve the security of their network in order to ensure the protection of personal data. It also grants to the data owner the right of access to such data without cost, to update his/her own data, as well as request its elimination or annulment.

If the constitutional rights of data owners are not respected, those affected may file habeas data actions, in accordance, with Article 50 of the Organic Law of Jurisdictional Guarantees and Constitutional Control.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

Currently, Ecuador does not have a specific law regulating marketing communications, but it is expected that once the Bill for Personal Data Protection is approved, a specific regulation on this matter will be developed by the Personal Data Authority.

8.2 How is the use of tracking technologies (eg, cookies, pixels, sdks) regulated from a privacy perspective?

As stated above, this is not currently regulated Ecuador but a specific regulation is expected to be developed when the Bill on Personal Data Protection is approved by the Assembly.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

There is no current regulation on the matter.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook custom audiences or via LiveRamp) ?

The only clear limit that has been defined in the Ecuadorian legal system on personal data is the consent of the owner for collection, use and transfer of personal data. This means that, currently, advertisers require express authorization to share a person's data for customer matching.

However, the Bill is more permissive, as it states exceptions from the need to obtain the owner's consent for transferring data, such as when the data has been collected from sources accessible to the public, or when the data treatment corresponds to the legal relationship between the data owner and the data controller.

8.5 Are there specific privacy rules governing data brokers?

There is no current regulation on the matter.

8.6 How is social media regulated from a privacy perspective?

There is no current regulation on the matter; all provisions focus more on the constitutional right of intimacy of the person.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

There is no current specific regulation on the matter. However, it is not possible to collect, use, process or transfer any personal data for any purpose without the authorization of the owner.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

Currently, any data transfer requires the express consent of the owner, according to the Constitution. Hence, the first restriction is the consent of the owner, which must given be prior to transfer and expressly specify the information that is being authorized to be transferred.

However, in Article 48 of the Bill, exceptions are set out when the consent of the holder for the transfer or communication of personal data will not be required. These include, among others:

(a) when the data has been collected from sources accessible to the public,

(b) when personal data must be provided to an administrative or judicial authority, and

(c) personal data related to health necessary to solve an emergency.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

The main consideration for companies is consent of the data owners. In addition, the Bill establishes that the processing of personal data that is carried out by third parties must be regulated by contract, that clearly and precisely establishes that the data processor will treat the personal data according to the instructions of the data controller and that data will not be used for purposes other than those stated in the contract.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

As mentioned above, there is no specific law in Ecuador that provides sanctions in cases of violation of the information and personal data of citizens. However, at present, the Comprehensive Organic Criminal Code establishes the following:

> "**Article 178 — Violation of privacy -** Any person who, without the legal consent or authorization, accesses, intercepts, examines, retains, records, reproduces, disseminates or publishes personal data, text, voice, audio and video messages, postal objects, information contained in computer media, private or confidential communications of another person by any means shall be subject to a custodial sentence of one to three years..."
>
> "**Article 229 — Illegal disclosure of database -** Any person who, for his own benefit or that of a third party, discloses registered information contained in files, archives, databases or similar media, through or directed to an electronic, computer, telematics or telecommunications system; voluntarily and intentionally materializing the violation of the secrecy, intimacy and privacy of persons, shall be punished with a custodial sentence of one to three years..."

Also, there is limited case law of damages awards based on *habeas data* resolutions if actual harm to the data owner is demonstrated.

10.2 Do individuals have a private right of action? What are the potential remedies?

In accordance with the Constitution of Ecuador and the Organic Law of Jurisdictional Guarantees and Constitutional Control, the owners of information and personal data that have been affected may file a habeas data action on their own rights the same regarding the couple of criminal regulations on the matter.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Ecuador which affect privacy?

There are no specific rules yet.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

The Bill for Personal Data Protection, as mentioned before, should be approved by the Assembly in the following months and will establish a complete and highly regulated legal frame for data processing.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Ecuador?

Not at this time.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

Data protection is a very new topic for Ecuador; it gained some relevance when it was included in the Constitution of 2008; however, it was never properly regulated. The lack of a specialized Law that clarifies the ambiguities in the dispersed laws and fills the legal voids is the main reason that led the proposed Bill in 2019.

Nevertheless, the massive data breaches which have been publicly reported demonstrate how carelessly data processing is being handled in the country and reveal the weakness of our security systems, and are the main trigger for the Bill to be finally presented to the Assembly.

My personal opinion is that this law is needed in Ecuador now with more urgency than ever before. Perhaps the Bill presented to the Assembly could be deemed a little over-regulatory; however, this is necessary for a country in which we have been absolutely unprotected.

12.2 What do you envision the privacy landscape will look like in 5 years?

I believe that the Bill is a response to the lot of legal gaps that exist in Ecuador on the processing of personal data. If the Bill is accepted and, subsequently, the creation of a Regulation of the Law of Protection of Personal Data is considered, the panorama in five years in Ecuador will be different. That is, the answers to data protection problems will be agile, clear and fast. The security measures for data protection will be effective, and, above all, there will be clear limits on the use and processing of personal information. The

country by then will most likely have a "formal" control of data processing and protection of privacy rights, which, of course, will still be imperfect due to the lack of experience of the Authority (to be created) and the compliance timeframes that will have to be granted to the companies.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

If the Bill is approved, the establishment of responsibilities and roles (data controllers and delegates) for processing personal data will definitely represent challenges for companies. This because, as there is a specific rule that regulates the responsibilities of each of the subjects involved, it means that companies will have to use more resources to comply with these legal requirements, which they are not used to. Likewise, investment in better developed terms and conditions of use, security measures and registration of data bases will be new challenges for companies in Ecuador.