Hospedaje Transfronterizo de Datos

TENDENCIAS, Legalidad y prudencia

Hospedaje Transfronterizo de Datos

principales problemas

1. "… restrictions on legitimate cross-border information flows. Countries around the world are increasingly employing a host of measures to exclude or discriminate against foreign information, information services or technology." (1)
2. "… local Infrastructure or investment mandates. A variety of countries have introduced or enacted measures that would compel financial services providers to process data on-shore or require online service providers or other companies to locate physical infrastructure such as servers within their borders." (1)
3. "… uncertainty concerning which legislation is applicable…" (2)
4. " … when and how governments can access users' data." (3)

Fuente: **(1) Promoting Cross Border Data Flows: Priorities for the Business Community**

(2) How Borderless is the Cloud? – Kommerskollegium National Board of Trade (Swe

(3) A Global Reality: Governmental Access to Data in he Cloud – A Hogan Lovells Wh

EXPERTOS

- "The main impediments for cloud services are therefore often the rules and laws which exist in different countries regarding how information may be handled and stored. For example, confidentiality legislation, data security laws, personal information laws as well as licensing and copying rules." (1)
- "But even in the USA, there is no comprehensive obligatory trans-sector regulation of data protection. Collection and usage of personal information in sectors which can be considered to be especially sensitive, such as the **health and financial sectors**, is regulated instead (Berry and Reisman, 2012). " (1)

Fuente: (1) How Borderless is the Cloud? – Kommerskollegium National Board of Trade (

EXPERTOS

- "... An Australian commissioner has instructed state government organizations to use only those cloud service providers that agree to comply with the state of Victoria's information privacy laws. Locally based data centers are preferred. By the same token, the New Zealand government issued a revenue alert in 2010 stating that any organization in that country wanting to utilize cloud computing must either use cloud services that have **data centers located within the country, or they must keep local copies of all records**.." (1)
- " … China, Indonesia, Vietnam, Brazil, Argentina, Chile, Colombia, Peru, and Costa Rica all have adopted or proposed rules that prohibit or significantly restrict companies from transferring personal information out of the domestic territory. In parallel, many markets are beginning to require that data centers be located inside their geographic borders." (2)

Fuente: **(1) Cloud Computing Concerns in the Public Sector - C**
(2) Lockout - BSA

EXPERTOS

"***Localization requirements***

... "localization requirements" that compel firms storing and processing data for clients from a given country to locate the data in that country. Governments typically create such requirements for the ostensible purpose of keeping data private and secure...

Localization requirements are most often associated with two industries: **finance and government**. For example, South Korea requires that financial institutions process data within South Korea unless clients provide written consent ..."

Fuente: Policy Challenges of Cross-Border Cloud Computing - United States International Trade C

EXPERTOS

Uncertainty regarding the applicable legal system

Since cloud suppliers want to optimize their capacity, data is often moved between different servers, depending on where storage space is available. When cloud services are being used for the processing of data it is also common for the information to be moved between servers. This means that even if there is an agreement with the customer about where the information shall be stored, it may be moved to another location during processing (i.e., even another country or continent) and then be returned and stored in the agreed location. The results are that, without being aware of it, a customer can be exposed to another country's legal system, regardless of whether the storage location is stated in the agreement. These types of technical aspects of how cloud computing functions are therefore of vital importance for the legal aspects. Situations can also arise where information stored in a certain country is by legal obligation made available to that country's authorities, such as police or intelligence authorities (Cloud Sweden 2010). As it is often ambiguous as to which country's legal system is applicable, two legal systems may end up in conflict with one another. There are currently no international agreements which regulate this.

The issue of the sovereignty of national data, *data sovereignty*, is central for states. This term is broader than confidentiality, for example, since it relates to the actual ownership rights to the information. When public data and systems are stored or processed in a server in a foreign country, central issues can arise such as the potential consequences of the information being exposed to another country's set of rules and regulations and its legal system. Public organizations and authorities are in general under extremely strict obligations to ensure that public IT systems as well as public information are protected.

Fuente: How Borderless is the Cloud? – Kommerskollegium National Board of Trade (Sweden)

Inseguridad global

Vsitazo a algunas reformas de protección de datos que se debaten en diferentes países.

UNIÓN EUROPEA

Los políticos han reanudado un llamado por una 'euronube', un sistema que garantizaría que los datos de ciudadanos europeos permanezcan en servidores europeos.

BRASIL

Acelera el voto sobre una ley que requiere que los datos de brasileños permanezcan en servidores del país.

FRANCIA

Apoya leyes más fuertes de protección de datos que incluye métodos para transferir información hacia países por fuera de la UE y una nueva autoridad de privacidad de datos.

INDIA

Planea prohibir a funcionarios gubernamentales el uso de servicios de e-mail estadounidenses, como Gmail y Yahoo.

ALEMANIA

Ha pedido a la UE que cancele los acuerdos de intercambio de datos con EE.UU. Deutsche Telekom y otras empresas han lanzado servicios llamados "E-mail hecho en Alemania", con el fin de atraer usuarios de Gmail y Yahoo.

Fuentes: UE; los países

The Wall Street Journal

en el mundo ...

País	Exigen Servicios Locales	Preferencia Servicios Locales	Certifica por Territorio
Argentina			◑ ◑
Australia	◑	◑ ◑ ◑	✔ ◑
Brazil		◑	
China	◑	◑	◑
Francia	◑	◑ ◑	✔
Alemania		◑	◑ ✔
India	✔	✔	
Indonesia	◑	◑	✔ ✔
Italia	✔	✔	✔
Malaysia			◑
Mexico	✔	✔	✔
Rusia			

◑ : Existencia de inconsistencias o vacíos legales

✔ : Existencia de restricciones explícitas

nte: BSA 2013 Global Cloud Computing
recard

en el mundo...

Australia	The government presented a bill in November 2011 that would require local data centers for the personally controlled e-health record system.
Brunei	Brunei has data residency laws, meaning that companies can store the data they collect only on servers in country.
China	China has local data server requirements due to national security, currency control and industrial policy. China has also put in place an array of laws and regulations that establish a local entity, China UnionPay (CUP), as the monopoly network for processing RMB-denominated transactions in China.[2] The United States is currently challenging the CUP monopoly in the World Trade Organization. If the United States prevails, then it must ensure that China does not seek to perpetuate the entrenched position of CUP by imposing a local data server requirement. China has data residency laws that declare companies can store the data they collect only on servers in country.
Greece	In February 2011, Greece passed a law that states, in part, "Data generated and stored on physical media, which are located within the Greek territory, shall be retained within the Greek territory." The European Commission has criticized this action by Greece as inconsistent with the E.U. single market, but the rule remains in effect.

Ejemplos de restricción de localización de datos

India	The government has proposed a measure that would require companies to locate part of their IT infrastructure within the country to provide investigative agencies with ready access to encrypted data on their servers. This measure also will require that data of Indian citizens, government organizations and firms hosted on the servers of these companies not be moved out of the country. Failure to comply with this rule will be a criminal offence and company officials will face prosecution.
Indonesia	In 2009, the Ministry of Communication and Information Technology of the Republic of Indonesia proposed a draft government regulation to implement law no. 11 (2008) concerning electronic information and transactions. One of the provisions, article 25.3, stipulates that every electronic system's provider for public services that operates a data center is required to locate its data center and disaster recovery center within the Indonesian territory. This draft regulation will become law if it is "harmonized" with the Ministry of Justice and the Ministry of Economic Affairs.
Malaysia	Malaysia passed a local data server requirements law but has not yet implemented it.
Nigeria	Nigeria has adopted Guidelines on Point-of-Sale Card Acceptance Services, which require that all point-of-sale and ATM domestic transactions be processed through a local switch (essentially, a server) and prohibit routing of transactions for processing outside the country. The guidelines also require centralized switching of domestic transactions.
Russia	Russia has adopted legislation requiring that infrastructure necessary to core payment processing services be located on the territory of the Russian Federation.
South Korea	The Financial Services Commission is considering regulations that would require insurance companies to maintain servers in country for company financial data and restrict transfers of such data (not pertaining to policy holders or employees) outside of South Korea's borders. This is despite provisions in the KORUS Free Trade Agreement, scheduled to take effect two years from entry into force. The free trade agreement permits the sending of data across the border intra-company or to third parties. The data transfer provision was intended to establish an innovative precedent in Asia, thereby allowing U.S. financial services companies to integrate regional and global operations by using established data processing hubs.
Ukraine	Ukraine is considering laws and regulations that would establish a domestic monopoly for processing domestic payment transactions and exclude foreign networks from providing processing services.
Venezuela	Venezuela has local data server requirements due to currency control for debit transactions. Venezuela has adopted a law that effectively requires in-country processing of domestic payment transactions.
Vietnam	Vietnam has data residency laws, meaning that companies can store the data they collect only on servers in country.

Fuente: The Growing Threat of Local Data Server Requirements - Business Roundtable

en el mundo ...

GOVERNMENTAL AUTHORITIES' ACCESS TO DATA IN THE CLOUD: A COMPARISON

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
Australia	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Canada	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Denmark	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
France	Yes	Yes, except for personal data without a legal purpose, electronic communications	No	Yes	Yes	Yes
Germany	Yes	Yes, except for personal data without a legal purpose, electronic communications	Yes, except may withhold until disclosure no longer would compromise the investigation or in investigation of serious criminal offenses, national security, or terrorism	Yes	Yes	No, not without cooperation from the other country's government, except for telecommunications customer non-content data
Ireland	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Japan	Yes	No – must request data through legal process	No	Yes	Yes	No, not without cooperation from the other country's government**
Spain	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United Kingdom	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes	Yes

Países que permiten ver datos localizados en él que pertenecen a otros países

Fuente: A Global Reality: Governmental Access to Data in the Cloud – A Hogan Lovells White Paper

En Estados unidos

... the United States only regulates the collection and use of personal data in certain sensitive sectors, such as **healthcare** (under the Health Insurance Portability and Accountability Act, or HIPAA) and **financial services** (under the Gramm-Leach-Bliley Act). (1)

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes	Yes

(2)

uente: (1) Policy Challenges of Cross-Border Cloud Computing - United States International Trade Co
(2) A Global Reality: Governmental Access to Data in the Cloud – A Hogan Lovells White Pape

En Estados unidos

European Union

The EU Data Privacy Directive establishes standards that member states must follow in their domestic data privacy laws. These standards apply anytime someone (whether a company or an individual) collects personal data that can be linked to a specific individual (an EU citizen). Data collection or processing that does not meet the standards is prohibited (box 1).

These standards apply to all personal data. Examples include internal personnel records that employers keep on their EU employees and online travel booking systems accepting reservations from EU customers.

The Directive has far-reaching international implications. As implied in these examples, U.S. firms must comply with the Directive whenever they possess personal data involving EU citizens. In fact, not all U.S. firms may legally possess this data. The EU prohibits export of personal data unless the importing country "ensures an adequate level of protection" as certified by the EU Commission. **The United States is not among the nine countries that have been recognized.**

Fuente: Policy Challenges of Cross-Border Cloud Computing - United States International Trade C

En Estados unidos

CLOUD COMPUTING: AN OVERVIEW OF THE TECHNOLOGY AND THE ISSUES FACING AMERICAN INNOVATORS

==========

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

_____

JULY 25, 2012

_____

Serial No. 112-122

_____

En Estados unidos

Participan:

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, Chairman

F. JAMES SENSENBRENNER, Jr., Wisconsin	JOHN CONYERS, Jr., Michigan
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. ``BOBBY'' SCOTT, Virginia
DANIEL E. LUNGREN, California	MELVIN L. WATT, North Carolina
STEVE CHABOT, Ohio	ZOE LOFGREN, California
DARRELL E. ISSA, California	SHEILA JACKSON LEE, Texas
MIKE PENCE, Indiana	MAXINE WATERS, California
J. RANDY FORBES, Virginia	STEVE COHEN, Tennessee
STEVE KING, Iowa	HENRY C. ``HANK'' JOHNSON, Jr., Georgia
TRENT FRANKS, Arizona	PEDRO R. PIERLUISI, Puerto Rico
LOUIE GOHMERT, Texas	MIKE QUIGLEY, Illinois
JIM JORDAN, Ohio	JUDY CHU, California
TED POE, Texas	TED DEUTCH, Florida
JASON CHAFFETZ, Utah	LINDA T. SANCHEZ, California
TIM GRIFFIN, Arkansas	JARED POLIS, Colorado
TOM MARINO, Pennsylvania	
TREY GOWDY, South Carolina	
DENNIS ROSS, Florida	
SANDY ADAMS, Florida	
BEN QUAYLE, Arizona	
MARK AMODEI, Nevada	

Richard Hertling, Staff Director and Chief Counsel
Perry Apelbaum, Minority Staff Director and Chief Counsel

Subcommittee on Intellectual Property, Competition, and the Internet

BOB GOODLATTE, Virginia, Chairman

BEN QUAYLE, Arizona, Vice-Chairman

F. JAMES SENSENBRENNER, Jr., Wisconsin	MELVIN L. WATT, North Carolina
HOWARD COBLE, North Carolina	JOHN CONYERS, Jr., Michigan
STEVE CHABOT, Ohio	HOWARD L. BERMAN, California
DARRELL E. ISSA, California	JUDY CHU, California
MIKE PENCE, Indiana	TED DEUTCH, Florida
JIM JORDAN, Ohio	LINDA T. SANCHEZ, California
TED POE, Texas	JERROLD NADLER, New York
JASON CHAFFETZ, Utah	ZOE LOFGREN, California
TIM GRIFFIN, Arkansas	SHEILA JACKSON LEE, Texas
TOM MARINO, Pennsylvania	MAXINE WATERS, California
SANDY ADAMS, Florida	HENRY C. ``HANK'' JOHNSON, Jr., Georgia
MARK AMODEI, Nevada	

Blaine Merritt, Chief Counsel
Stephanie Moore, Minority Counsel (Ctrl)

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

OPENING STATEMENT: The Honorable **Bob Goodlatte**, a Representative in Congress from the State of Virginia, and Chairman, Subcommittee on Intellectual Property, Competition, and the Internet.

"We need to ensure that as this new American technology sector grows, it is able to compete on a level playing field abroad and to promote U.S. innovation technology and jobs."

OPENING STATEMENT: The Honorable **Lamar Smith**, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary.

"Cloud computing relies on the seamless flow of data across borders and international interoperability. Unfortunately, some countries have adopted rules that limit the specific types of data that can leave their borders, and have put in place restrictive regulatory frameworks.

Some countries also have spread deliberate misinformation about U.S. laws, like the PATRIOT Act, saying that it negatively affects the security and privacy protections that U.S. cloud providers offer compared to European providers. These actions hurt the competitiveness of American companies and cost Americans jobs."

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

PREPARED STATEMENT: The Honorable **Melvin L. Watt**, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Intellectual Property, Competition, and the Internet.

“There are multiple layers of privacy concerns as well. Although I am sympathetic to the barriers companies are facing internationally due to other countries' perceptions of our privacy laws, I am more concerned with the consumer's right to privacy within the cloud. While I continue to believe that consumer privacy is paramount, the cloud offers new and innovative ways for the technologically savvy criminal to exploit the cloud for nefarious purposes. The ``Backpage'' prostitution scandal with Craigslist is just one example. The cloud must develop with caution to ensure that illegality does not flourish within the cloud, and Congress should update the Electronic Communications Protection Act (ECPA) to provide clear guidance on when and how law enforcement is entitled to access otherwise private data and communications.”

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

WITNESS: **Robert W. Holleyman**, II, President and Chief Executive Officer, Business Software Alliance (BSA)

- "Other countries are doing everything they can to knock us off the block."
- "Because the stakes are so high, and because of U.S. cloud companies' early leadership, some countries are taking policy steps to shut us out of their markets. The stakes of this are enormous, and if we want to get things right and to continue leading in the cloud, there is an urgent need for Congress and the Administration to forge an open and competitive global landscape."
- "Some countries are even adopting rules that would explicitly prevent the transfer of personal information outside their borders. Now these are bad signs for the global economy, but especially for America since we are so heavily dependent on selling products and services overseas."
- "... this Committee can take a lead role in reforming the Electronic Communications Privacy Act, ECPA. In the cloud era, digital files should be subject to the same laws and protections as paper files. And finally, we need to dispel myths about the PATRIOT Act. Foreign governments are scaring customers away from U.S. cloud services by portraying our law as unusually invasive. The fact is every government has authority to access data to protect national security, and everyone needs to understand that."

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

WITNESS: **Justin Freeman**, Corporate Counsel, Rackspace US, Inc.

"Concerns about privacy and security of data have become heightened as businesses hand off their data to systems in the cloud. And they are a major barrier to the competitiveness of American cloud companies internationally. Concerns about data privacy limits, the willingness of foreign companies to do business with United States firms, and threatening to exclude American companies from competing abroad.

The lack of international privacy standards is a growing source of distrust amongst regulatory agencies seeking to enforce their domestic laws, and businesses struggling to ensure their compliance. There is a perception, even if unfounded, that U.S. privacy protections are insufficient to protect the data which is stored either on U.S. soil or with U.S. companies. This concern results in a reluctance by foreign companies to do business with U.S. cloud companies, and we increasingly see regulatory authorities, especially in the EU and European economic area, moving in the direction of denying U.S. cloud providers access to the European market."

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

WITNESS: **Daniel Chenok**, Executive Director, Center for the Business of Government, International Business Machines Corporation (IBM)

"The extent to which government can access data across borders can be a subject of confusion among cloud providers and users. However, as has been indicated today, many nations have similar domestic data policies. A recent white paper from the law firm Hogan Lovells found that each of the 10 countries studied vests authority in the government to require a cloud service provider to disclose customer data in certain situations..."

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

WITNESS: **Daniel Castro**, Senior Analyst, Information Technology and Innovation Foundation (ITIF)

- "...one important issue is addressing the complex jurisdictional questions that arise from having data subjects, data owners, and service providers under different legal jurisdictions and facing conflicting regulations."

- "One important step Congress can take in this direction is to update the laws that govern the electronic surveillance of data. The Electronic Communications Privacy Act was enacted in 1986, and has not kept pace with the advancement of technology and the growth of cloud computing."

- "Some countries are using data security and data privacy regulations to create geographic restrictions on where cloud computing service providers can store and process data. Other countries have policies that explicitly require cloud computing service providers to operate data centers domestically...

  Localization requirements also serve as a form of protectionism for domestic cloud computing providers since it may not be economically viable for a foreign competitor to build a domestic data center. Examples of this type of behavior can be found in many countries, for example, Greece, Vietnam, and Brunei have all passed laws which require data generated within the country to be stored on servers within those countries. Both the Norwegian and the Danish protection authorities have issued rulings to prevent the use of certain cloud computing services when those servers were not located domestically...

  ... the U.S. government should affirm its intention to refrain from imposing its own local data center requirements. These policies may be tempting, but they diminish the capacity of the United States to hold other countries accountable for similar forms of protectionism."

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

PREGUNTAS Y RESPUESTAS: **Mr. Watt**, the gentleman from North Carolina

“The question is, how do we protect ourselves, how do we protect our own consumers' information without those kinds of barriers in our own country? And if we put them up in our own country, does that not incentivize other countries to put them up there? The same thing with national security concerns. If we are allowing our national security apparatus access to

information in the cloud, would it not be a legitimate concern for other countries to be concerned about the extent to which our national security apparatus would have access to their information in the cloud?”

“Mr. Holleyman. I will start by saying, hey, look, I think we need to do both simultaneously. I mean, there are some gaps in U.S. law that we think need to be resolved, like the need for ECPA reform that would ensure some greater levels of privacy for data that is stored in the cloud. And that would be an important signal for other countries.”

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

En Estados unidos

PREGUNTAS Y RESPUESTAS: **BOB GOODLATTE**, Virginia, Chairman

“Mr. Holleyman and Mr. Freeman, what are some of the more egregious market access issues that BSA or Rackspace or other businesses have found foreign countries engaging in against American cloud computing companies in the European Union or in countries like Canada, Australia, India, Japan, China? As I prepared this question, it seemed to have gotten longer. We will start with you, Mr. Holleyman.

“Mr. Holleyman. ... you have the concerns I see happening in Germany where German government officials are talking about the fact that all German data should be stored in Germany, both high sensitive and low sensitive and medium sensitive data, not only for the German government, but for German citizens. And then you have a marketing campaign by Deutsche Telecom, which is effectively a third owned by the German government, that is invoking the PATRIOT Act and citing the PATRIOT Act as a reason why customers should use Deutsche Telecom's hosting services over U.S. providers.**”**

“Mr. Freeman. That sort of fear, uncertainty, and doubt I think inform Canada's FOIPA law, which is a good example of a protectionist measure that excluded U.S. participation in the marketplace. Canada passed a patient privacy bill that prohibited the storage of any patient health information on any server located in the United States based on this sort of fear and uncertainty...”

Fuente: Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators - Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the

Grandes operadores

Google Informe de transparencia

Solicitudes de los Estados Unidos (ECPA)

¿Qué tipo de solicitudes legales recibe Google de los organismos gubernamentales de los EE. UU.?

Las más habituales son, con diferencia, las citaciones, seguidas de las órdenes de búsqueda. Un estatuto federal llamado Ley de Privacidad en las Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA), regula el modo en que los organismos gubernamentales pueden utilizar estos tipos de procesos legales para obligar a empresas como Google a revelar información sobre los usuarios. Esta ley se aprobó en 1986, antes de que la Web, tal y como la conocemos hoy, existiera. No ha podido seguir el ritmo del uso que las personas hacen de Internet actualmente. Esta es la razón por la que hemos trabajado con muchos grupos de defensa de la privacidad y empresas, entre otros, a través de la Coalición para el Proceso Digital Adecuado (Digital Due Process Coalition), para que esta ley tan importante se actualice y te pueda garantizar el nivel razonable de privacidad que puedes esperar cuando utilizas nuestros servicios.

Grandes operadores

Google Informe de transparencia

Solicitudes de fuera de los Estados Unidos

¿Cómo responde Google a las solicitudes de organismos gubernamentales de fuera de los Estados Unidos?

Por medio del Tratado de Asistencia Legal Mutua (MLAT) y otros acuerdos diplomáticos y de cooperación, los organismos de fuera de los EE. UU. pueden trabajar con el Departamento de Justicia de los EE. UU para reunir pruebas para investigaciones legítimas. En algunos casos, la Comisión Federal de Comercio de los EE. UU. puede ofrecer asistencia.
Si la legislación de los EE. UU. está implicada en la investigación, puede que un organismo de los EE. UU. abra su propia investigación y proporcione las pruebas que reúna a investigadores de fuera de los EE. UU. También es posible que Google revele datos en respuesta a solicitudes de revelación urgentes cuando se considere que hacerlo es necesario para impedir que una persona muera o que sufra daños físicos graves.

De modo voluntario, podemos proporcionar datos de los usuarios en respuesta a procesos jurídicos válidos de organismos gubernamentales de fuera de los EE. UU. siempre que estas solicitudes se realicen de acuerdo con las leyes internacionales, la legislación de los EE. UU., las políticas de Google y la legislación del país solicitante.

¿Qué es un Tratado de Asistencia Legal Mutua (MLAT)?

Un MLAT es un tratado entre los EE. UU. y otro país que define la forma en que cada país ayudará a otro en asuntos legales, como por ejemplo en investigaciones penales. A través de un MLAT, un gobierno de otro país puede pedir al gobierno de los EE. UU. que le ayude a obtener pruebas de entidades de los EE. UU., incluidas empresas como Google. Si el gobierno de los EE. UU. aprueba la solicitud, Google responderá a ella.

¿El MLAT es la única forma en que los gobiernos de fuera de los EE. UU. pueden obtener información de empresas de los EE. UU.?

No. Además del MLAT, hay muchas formas en que otros países pueden obtener información de empresas como Google, como por investigaciones conjuntas entre los EE. UU. y las autoridades locales encargadas de la aplicación de las leyes o solicitudes de revelación urgentes, entre otras.

Grandes operadores

Google Informe de transparencia

¿Cómo funciona el Tratado de Asistencia Legal Mutua (MLAT, Mutual Legal Assistance Treaties)?

El proceso del Tratado de Asistencia Legal Mutua (MLAT, por sus siglas en inglés) es bastante simple. Un ejemplo hipotético sería: un policía de Londres está investigando un caso de robo de identidad y tiene pruebas de que el culpable tiene una cuenta de Gmail en particular. Para continuar con su investigación, el agente necesita saber quién es el usuario. Debido a que existe un MLAT entre el Reino Unido y los Estados Unidos, el policía puede pedirle al Ministerio del Interior del Reino Unido que le solicite información a la Oficina de Asuntos Internacionales del Departamento de Justicia de los Estados Unidos. El Departamento de Justicia de los Estados Unidos traslada la solicitud a la oficina del Fiscal de Estados Unidos correspondiente, quien se ocupa del proceso legal de los Estados Unidos y entrega la solicitud de datos de usuario a Google. Si la solicitud cumple con la ley y las políticas de Google, proporcionaremos la información a la oficina del Fiscal de Estados Unidos, y desde allí llegará al policía del Reino Unido.

Grandes operadores

Microsoft

Microsoft's Law Enforcement Requests Report for the first six months of 2013

What is the process for disclosing customer information to law enforcement?

Both Microsoft and Skype require an official, signed document, issued pursuant to local law and rules to be delivered to our compliance teams based in the U.S. and Ireland for Microsoft data and Luxembourg for Skype.

For law enforcement requests for Microsoft customer data from non-English speaking countries, a local team or individual, typically a lawyer or someone operating under legal guidance will receive and authenticate the law enforcement request. If it complies with local law, then it will be translated and sent to the Microsoft compliance teams in the U.S. or Ireland. Skype's compliance team members speak multiple languages and assess the validity of most requests, especially those from European law enforcement entities, sent directly to the team in Luxembourg, which is the same procedure Skype employed prior to the Microsoft acquisition.

What laws apply to Microsoft and Skype customer records and content? (ECPA)

For data hosted in the U.S., Microsoft follows the Electronic Communications Privacy Act. We require at least a subpoena before turning over non-content records, such as basic subscriber information or IP connection history and we require an order or warrant before producing content. Irish law and European Union directives apply to the Hotmail and Outlook.com accounts hosted in Ireland. Skype is a wholly-owned, but independent division of Microsoft, headquartered in and operating pursuant to Luxembourg law.

How does Microsoft and Skype determine what law enforcement entities are able to request data?

Microsoft must produce data in response to valid legal requests from U.S. and Irish law enforcement entities because we are headquartered in those jurisdictions or because we host data in those countries. Microsoft may disclose non-content data pursuant to a law enforcement request after it is validated locally and transmitted to our compliance teams in the U.S. and Ireland. Skype must produce data to Luxembourg authorities and is able to disclose some records to law enforcement entities outside of Luxembourg.

Grandes operadores

Transparency Report

TWITTER

Guidelines for Law Enforcement

Requests From Non-U.S. Law Enforcement

U.S. law authorizes Twitter to respond to requests for user information from foreign law enforcement agencies that are issued via U.S. court either by way of a mutual legal assistance treaty ("MLAT") or a letter rogatory. It is our policy to respond to such U.S. court ordered requests when properly served.

Non-U.S. law enforcement authorities may also submit requests for emergency disclosure under exigent circumstances, as outlined in the section titled "How to Make an Emergency Disclosure Request," above.

Grandes operadores

facebook

Informe de solicitudes de gobiernos Preguntas más frecuentes

Información para las autoridades del orden público

Requisitos de procesos jurídicos en EE.UU.
Sólo revelamos los registros de las cuentas según nuestras condiciones del servicio y la legislación aplicable, incluida la ley estadounidense de almacenamiento de datos federal (Stored Communications Act, SCA), 18 U.S.C., secciones 2701-2712. En virtud de la ley de EE. UU.:

Requisitos para procesos legales internacionales (MLAT)
La revelación de registros de una cuenta sólo puede hacerse de conformidad con nuestras condiciones de servicio y la ley pertinente. Para exigir la revelación de contenido de una cuenta, es posible que se requiera presentar una solicitud de asistencia judicial mutua o un exhorto. Más información en: facebook.com/about/privacy/other.

U.S. DEPARTMENT OF STATE

DIPLOMACY IN ACTION

2012 INCSR: Treaties and Agreements

BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS

2012 International Narcotics Control Strategy Report (INCSR)

Report

March 7, 2012

Share

Treaties

Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and related matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners. MLATs, which are negotiated by the Department of State in cooperation with the Department of Justice to facilitate cooperation in criminal matters, are in force with the following countries: Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Germany, Greece, Grenada, Hong Kong, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, the Kingdom of the Netherlands (including Aruba, Bonaire, Curacao, Saba, St. Eustatius and St. Maarten), Nigeria, Panama, Philippines, Poland, Romania, Russia, St. Lucia, St. Kitts & Nevis, St. Vincent & the Grenadines, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Trinidad & Tobago, Turkey, Ukraine, United Kingdom (including the Isle of Man, Cayman Islands, Anguilla, British Virgin Islands, Montserrat and Turks and Caicos), Uruguay, and Venezuela. In addition, on February 1, 2010, 27 U.S.-EU Instruments/Agreements/Protocols entered into force that either supplement existing MLATs or create new mutual legal assistance relationships between the United States and every member of the EU. Mutual legal assistance agreements have been signed by the United States but not yet brought into force with the following countries: Algeria, Bermuda, and Colombia. The United States is engaged in negotiating additional MLATs with countries around the world. The United States also has signed and ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States, the United Nations Convention against Corruption, the United Nations Convention against Transnational Organized Crime, the International Convention for the Suppression of the Financing of Terrorism, and the 1988 UN Drug Convention.

Costa Rica no tiene un MLAT con USA

Grandes operadores

facebook

Solicitudes de datos

Datos de I Semestre 2013

Descargar como CSV

País	Total de solicitudes	Usuarios / Cuentas solicitadas	Porcentaje de solicitudes en las que se entregaron datos
Costa Rica	4	6	0 %

Hospedaje Transfronterizo de Datos

Definiciones - ley 8968

- **Base de datos:** Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

- **Datos personales:** cualquier dato relativo a una persona física identificada o identificable.

- **Datos personales de acceso irrestricto:** los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

- **Datos personales de acceso restringido:** los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

- **Datos sensibles:** información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

DEFINICIONES – LEY 8968

- **<u>Deber de confidencialidad:</u> obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.**

- **<u>Interesado:</u> persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.**

- **<u>Responsable de la base de datos:</u> persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.**

- **<u>Tratamiento de datos personales:</u> cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.**

INFRAESTRUCTURA

- **Respecto al almacenamiento de los datos el numeral 10 de la Ley No 8968 preceptúa que:**

- ***"…No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos…"***

Análisis

- **Esta disposición normativa obliga a los organismos privados y públicos a garantizar la seguridad e integridad de los centros de tratamiento y procesamiento de datos.**

- **Un centro de tratamiento de datos hoy en día es un lugar o espacio físico en donde se localizan los equipos de cómputo con sus sistemas y programas de computación.**

- **Ese espacio físico debe garantizar la seguridad e integridad de la información que almacena, administra y procesa para un determinado organismo público o privado.**

- **La pregunta que debemos hacernos es *¿Qué significa el concepto de seguridad e integridad de un centro de tratamiento de datos?***

Análisis

- **Esto es lo que en Derecho Administrativo se denomina concepto jurídico indeterminado, que se debe definir conforme lo establece el artículo 16 de la Ley General de la Administración Pública que para efectos ilustrativos citamos** ***"…En ningún caso podrán dictarse actos contrarios a reglas unívocas de la ciencia o de la técnica, o a principios elementales de justicia, lógica o conveniencia…".***

- **Básicamente, la técnica y la ciencia informática y en sistemas, se ha encargado de delimitar los conceptos de seguridad e integridad de un centro de tratamiento y procesamiento de datos.**

- **En la jerga de los informáticos un centro de tratamiento de datos debe reunir una serie de condiciones físicas y lógicas para que los componentes de cómputo y de programación tengan un ambiente seguro y que garantice la integridad de los datos administrados y almacenados.**

- **Adicionalmente, cuando los centros de tratamiento y procesamiento de datos son almacenados por un organismo público existen normativas específicas en relación a la forma de guardar y garantizar la integridad de los datos e información almacenada.**

Análisis

- **Esto se encuentra regulado en la Ley 7202 (Ley del Sistema Nacional de Archivos) que complementa algunos alcances de la Ley 8968 en relación al procesamiento y tratamiento de datos según las competencias administrativas y públicas de la Administración Pública Centralizada y Descentralizada en concordancia con el artículo 6 de la Ley No 8454 (Ley de Certificados, Firmas Digitales y Documentos Electrónicos) que en lo que interesa dispone:**

- ***"…Gestión y conservación de documentos electrónicos. Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas. La transición o migración a soporte electrónico, cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá contar, previamente, con la autorización de la autoridad competente. En lo relativo al Estado y sus instituciones, se aplicará la Ley del Sistema Nacional de Archivos, Nº 7202, de 24 de octubre de 1990. La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación***

Análisis

- **La interrelación de estos preceptos normativos permite aclarar el concepto técnico de seguridad e integridad de los datos contenidos en una base de datos de soporte electrónico o informático ubicado en un centro de tratamiento o procesamiento de datos, amén de los conceptos y especificaciones técnicas de la ciencia o ingeniería informática o en sistemas.**

- **Una vez abordados estos temas generales y específicos debo atender la pregunta** ***¿si de acuerdo a nuestro ordenamiento jurídico le es permitido al Estado (Artículo 1º de la Ley General de la Administración Pública "…La Administración Pública estará constituida por el Estado y los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado…") ubicar las bases de datos en lugares fuera del territorio nacional (Artículo 60 de la Ley General de la Administración Pública "…1. La competencia se limitará por razón del territorio, del tiempo, de la materia y del grado. 2. Se limitará también por la naturaleza de la función que corresponda a un órgano dentro del procedimiento administrativo en que participa…")?*****, es decir, físicamente fuera del territorio costarricense.***

Análisis

- **A la luz de la Constitución Política y de la normativa citada la respuesta a esta pregunta <u>es de ámbito negativo o restrictivo.</u>**

- **Para establecer esta afirmación debemos tomar en consideración que mucha de la información que almacenan, usan y administran las instituciones públicas tiene el carácter de sensible o restringida y en otros casos aunque la información sea irrestricta también por la naturaleza de la función pública (competencia territorial) de dichas instituciones la misma reviste de un carácter de seguridad estatal o de seguridad jurídica. (Artículo 1º de la Ley No 7494 –LCA-)**

Análisis

- **Este ejemplo es congruente con lo estipulado en el artículo 8 de la Ley 8968 al disponer que:**

- ***"…Los principios, los derechos y las garantías aquí establecidos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando se persigan los siguientes fines: a) La seguridad del Estado. b) La seguridad y ejercicio de la autoridad pública. c) (…) d) (…) e) La adecuada prestación de los servicios públicos. f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales…"*, es decir, se limita el Derecho Fundamental a la Autodeterminación Informativa no así las obligaciones de seguridad e integridad que deben tener los centros de procesamiento y tratamiento de datos, ni las competencias territoriales y funcionales del Estado.**

Análisis

- *¿Qué garantías podría tener una institución pública que contrata el almacenamiento de datos públicos (irrestricto, restringido y sensible) a una empresa que tiene físicamente los componentes de infraestructura fuera del ámbito de competencia territorial?*

- **Ante un conflicto con el proveedor o contratista qué potestades o competencias territoriales podrá hacer valer la institución pública en un territorio ajeno a la jurisdicción del contratante. La respuesta es obvia, no tiene ninguna potestad y competencia salvo los instrumentos jurídicos que establece el derecho internacional público y privado, esa situación sería una infracción al principio de competencia territorial de las potestades públicas.**

Análisis

- **Entendido lo anterior, la Ley No 8968 en sus artículos 27, 28, 29, 30, 31 y 32 crea y estatuye el régimen sancionador.**

- **En este régimen sancionador, el legislador <u>estableció como falta gravísima</u> la conducta o acto de** ***"…a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 3 de esta ley. (…) f) <u>Transferir, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares</u>…"***

- **En estos supuestos de hecho, ninguna institución pública podría trasladar información o datos personales (irrestricto, restringido o sensible) a ningún otro país, dado que implicaría renunciar a una potestad irrenunciable, recordemos que la LCA tiene ámbito territorial. En virtud de contrato administrativo no se podría trasladar bajo ninguna circunstancia datos personales para que sean almacenados en otros país, únicamente si se cuenta con**

Análisis

- **Finalmente, decimos que la respuesta debe ser de alcance restringido entendiendo que en el Derecho Comparado para que una institución pública pueda almacenar o colocar datos personales que competencialmente deben ser tratados en territorio costarricense es necesario la existencia de un convenio, tratado o acuerdo internacional que permita a dos Estados o varios Estados disponer de un régimen jurídico de cooperación para ubicar centros de tratamiento y procesamiento de datos de bases de datos de gestión pública.**

- **Por ejemplo en Europa entre los distintos países de la Unión Europea y al existir un mercado común entre los distintos países se han establecido disposiciones y normativas europeas para facilitar el tratamiento de datos personales entre los distintos países. Sin embargo, no se debe perder de vista el tema de la seguridad estatal y competencial público.**

- **La Administración Pública a la hora de contratar servicios en la Nube "Cloud Computing" no puede perder de vista estos aspectos y alcances normativos.**

Análisis

- **En ese sentido, el Estado no está facultado para establecer relaciones contractuales con proveedores que no garanticen la seguridad e integridad en el procesamiento y tratamiento de los datos de conformidad con las normas técnicas aplicables a esos sistemas y la ubicación física y geográfica de esos centros de tratamiento y procesamientos de datos debe estar en territorio costarricense de conformidad con el principio de competencia y seguridad jurídica.**

Conclusiones

- **El Estado no está facultado para establecer relaciones contractuales con proveedores o contratistas que no garanticen la seguridad e integridad en el procesamiento y tratamiento de los datos de conformidad con las normas técnicas aplicables a esos sistemas.**

- **La ubicación física y geográfica de esos centros de tratamiento y procesamientos de datos debe estar en territorio costarricense de conformidad con el principio de competencia y seguridad jurídica.**

- **Para que el centro de tratamiento y procesamiento de datos de una institución pública pueda estar localizado fuera del territorio costarricense se requiere de un acuerdo, tratado o convenio internacional que así lo permita, siempre y cuando, no se afecten principios constitucionales de seguridad jurídica y los derechos fundamentales de los costarricenses (autodeterminación informativa)**

Una reflexión muy importante

La Ley No 8422 (Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública)

Artículo 5º—Fraude de ley. La función administrativa ejercida por el Estado y los demás entes públicos, así como la conducta de sujetos de derecho privado en las relaciones con estos que se realicen al amparo del texto de una norma jurídica y persigan un resultado que no se conforme a la satisfacción de los fines públicos y el ordenamiento jurídico, se considerarán ejecutadas en fraude de ley y no impedirán la debida aplicación de la norma jurídica que se haya tratado de eludir.

Artículo 6º—Nulidad de los actos o contratos derivados del fraude de ley. El fraude de ley acarreará la nulidad del acto administrativo o del contrato derivado de él y la indemnización por los daños y perjuicios causados a la Administración Pública o a terceros. En vía administrativa, la nulidad podrá ser declarada por la respectiva entidad pública o por la Contraloría General de la República, si la normativa que se haya tratado de eludir pertenece al ordenamiento que regula y protege la Hacienda Pública. Si la nulidad versa sobre actos declaratorios de derechos, deberá iniciarse el respectivo proceso de lesividad, salvo lo dispuesto en el artículo 173 de la Ley General de la Administración Pública, Nº 6227, de 2 de mayo de 1978, en cuyo caso deberá actuarse de conformidad con lo allí establecido.

Artículo 58.—Fraude de ley en la función administrativa. Será penado con prisión de uno a cinco años, el funcionario público que ejerza una función administrativa en fraude de ley, de conformidad con la definición del Artículo 5 de la presente Ley. Igual pena se aplicará al particular que, a sabiendas de la inconformidad del resultado con el

Conclusiones

"…Unlike the United States and European Union (EU) which are largely homogenous regions from a jurisdiction standpoint, Asia Pacific is an extremely heterogeneous region. In the absence of international cloud computing legal and governance frameworks, cross-border data interchange will be nearly impossible in the government sector. Datacenters hosting the cloud infrastructure have to be largely local and preferably closer to the Federal agencies…"

"State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific" Published: 11 May 2011 By Arun Chandrasekaran & Mayank Kapoor

Fuente: http://www.frost.com/sublib/display-market-insight.do?id=232651031

Hospedaje Transfronterizo de Datos

SECTOR PRIVADO – BALANCE NECESARIO

NORMATIVA	CONSIDERACIONES LEGALES Y DE RIESGO EMPRESARIAL
LEY DEL CONSUMIDOR LEY DE COMPETENCIA LEY DE DATOS PERSONALES LEYES DE SEGURIDAD SOCIAL LEYES TRIBUTARIAS Y FISCALES LEYES SECTORIALES (SUGEF, SUGESE, SUGEVAL, BCCR, SUPEN, TRANSPORTE AEREO, TERRESTRE, ETC.)	CLIENTE (TITULAR DE LOS DATOS PERSONALES)
	JURISDICCION
	CONTINUIDAD DE NEGOCIO
	SEGURIDAD JURIDICA
	FISCAL, COMITÉ DE VIGILANCIA, AUDITORIAS
	JUNTA DIRECTIVA, GERENTE GENERAL, ASAMBLEA DE SOCIOS

Nuevo REGLAMENTO 37899-MEIC

Recientemente, el Estado por intermedio del Poder Ejecutivo emitió un nuevo Reglamento a la Ley No 7472 (Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor) en donde existe una serie obligaciones hacia las empresas del sector privado (especialmente del sector retail) en relación al manejo de información personal (clientes).

Estas nuevas obligaciones hacen necesario que el planteamiento de la ubicación territorial, física y de ambiente de estos datos no se limite a una cuestión de costo-beneficio, sino que existen otras consideraciones que las empresas deben plantearse en relación a la gestión de la información personal y a la operación de sus sistemas.

ARTICULO 229 REGLAMENTO LEY 7472

Información de planes de venta vigentes. Los comerciantes o proveedores que vendan o comercialicen ventas a plazo de bienes o de ejecución futura de servicios, deberán enviar a la DAC la información sobre los planes activos comercializados que incluya lo siguiente: nombre del consumidor, número de cédula del consumidor, tipo de plan, número de contrato de adhesión, monto del contrato de adhesión, número de cuotas totales, número de cuotas pagadas, monto pagado, monto por pagar, plazo del contrato de adhesión, fecha de inicio del contrato de adhesión y fecha de finalización del contrato de adhesión. Deberán garantizar que la administración cuente con la información actualizada en los medios que esta disponga para ello. En caso de incumplimiento se procederá de acuerdo con lo establecido en el artículo 242, 243 y 244 del presente reglamento.

Sector FINANCIERO

- **ACUERDO SUGEF 14-09 REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN**

Artículo 21. Tercerización de TI.

La entidad que contrate parte o la totalidad de uno o varios procesos o servicios de TI, relacionados con el procesamiento y almacenamiento de datos, independientemente del lugar en donde se lleven a cabo esas actividades, **debe mantener las bases de datos actualizadas y las aplicaciones vigentes físicamente en el territorio nacional**, accesibles por la SUGEF sin ningún tipo de restricción o condición.

La entidad supervisada es responsable de suministrar la información que le sea requerida por la SUGEF y proveer las facilidades para la ejecución de actividades de supervisión, indistintamente de que los procesos o servicios sean provistos por ella misma, otra empresa del grupo o conglomerado financiero o por un proveedor externo, o que sean llevados a cabo dentro o fuera del territorio costarricense.

Riesgo de negocio -

Hoy en día de acuerdo a la normativa revisada en esta exposición podemos afirmar que la decisión de ubicación geográfica (territorial) de una plataforma de servicios tecnológicos es una decisión que involucra riesgos para el negocio y que debe evaluarse desde los siguientes ángulos:

1) **Regulación específica aplicada al negocio, giro o actividad económica, el análisis del riesgo operativo no es un análisis exclusivo de las empresas del sector financiero;**

2) **Recurso humano (Recurso Experto en IT para evaluación de Sistemas y Contingencias)**

3) **Tercerización (Análisis de riesgo, Alcances Contractuales, Monitoreo, Subcontratación y Control)**

4) **Procesamiento de datos de acuerdo a la Ley de Datos Personales y Normativa Complementaria (Cumplimiento de buenas prácticas corporativas en materia de IT, hoy en día el *Compliance* no es exclusivo de sector financiero).**

5) **Criticidad de la información tercerizada y resolución de conflictos ¿Qué pasa si el proveedor no cumple? ¿Que pasa con el negocio? ¿Rescate del negocio? ¿quién tiene la responsabilidad desde el punto de vista del Gobierno Corporativo?**

LA DECISIONES DE TI DEBEN SER PRUDENTES

En conclusión la decisión de colocar los procesos de la empresa con un proveedor de servicios en la Nube que tenga su infraestructura fuera de territorio costarricense debe ser vista desde el punto de vista tecnológico, de riesgos operativos y continuidad de negocio y desde el punto de vista legal.

Reflexión

¿ES UN PROBLEMA TÉCNICO, EMPRESARIAL O JURÍDICO?