LACIGF 11

Wednesday 1 August, 15:00
Session 7 "Challenges in Managing Internet Identifiers"

A large group of participants met to discuss "Privacy under the GDPR approach and its impact on the DNS," a topic that was introduced by Rodrigo de la Parra, ICANN Vice President for Latin America and the Caribbean.

Rodrigo presented the GDPR's background, a topic that has been on ICANN's agenda and which deals with data protection and privacy measures for citizens and residents of the European Union.

This topic has become relevant to the technical community and, on this occasion, it was approached from a broader, not so technical focus so that it would be of greater interest to the community at large. Today, several questions were presented to the different working groups focusing not only on technical issues, but also on the implications of this issue for Internet governance.

Background

The GDPR came into force this past 25 May and its purpose is to protect EU citizens and residents against privacy violations and the misuse of personal data. "The regulation is an essential step to strengthen the fundamental rights of citizens in the digital era and to facilitate business by simplifying the rules in the Digital Single Market."

It applies to any company that processes and stores personal data belonging to subjects residing in the EU, regardless of the company's geographic location.

Failure to comply with the GDPR can result in fines of up to 20 million euros or 4% of a company's overall annual turnover. European data protection authorities are responsible for interpreting the events and enforcing the regulation, while European courts are responsible for resolving any dispute that may arise.

The GDPR is not very different from data protection laws or regulations that already exist in our countries.

But what does this have to do with the DNS, the Internet and ICANN?

ICANN is affected on two fronts:

First, internally. Just as any other organization that receives **personal data**, ICANN must be mindful of how these data are managed. This refers to data that is collected and processed to provide internal or external services.

But there is also a special dimension that affects ICANN's contracted parties, namely **domain name registries and registrars**, which follow the rules established by ICANN. Each time a registrant (whether an individual, a company or an organization) registers a domain name, they are asked to provide certain information, including personal data, which is collected in a public directory called the **WHOIS**. The WHOIS contains information on each domain: registry and registrar. Previously, it included data of a more personal nature. This WHOIS contradicts the EU regulation, which in turn affects any company that registers domains and maintains EU citizen data. About two years ago, the ICANN community began the process of discussing how to comply with the regulation while at the same time preserving the WHOIS directory. Bottom-up participatory discussions have been taking place in this sense.

As a result, Internet governance must address two major issues:

- Privacy and data protection on the Internet **vs**.

- Preserving the directory that is part of ICANN's mission, on the one hand, to maintain the technical and operational stability of the Internet, and on the other, to be able to provide information to court authorities.

For example, when investigating a crime related to a website, the legal system uses information contained in this directory to find the person or location where the network is used in a malicious manner.

Different Internet-related groups are discussing this topic, seeking to come up with a policy that defines its application.

The discussion on the WHOIS was already taking place, as some sectors were looking for a more robust WHOIS while others wanted a system that did not store sensitive information. The GDPR, however, accelerated this discussion among the community. As a result, a proposal emerged: the Temporary Specification for gTLD Registration Data, i.e., an interim model that guarantees a common framework for how gTLD registry data are managed. Meanwhile, the discussion among ICANN's different stakeholder groups continues in the hope of achieving a policy that defines how to continue using the WHOIS.

Some of the measures proposed included that replacing the single information layer for those who query the WHOIS with different layers (stratified model) depending on the level of information needed and in compliance with the GDPR. This means that only part of the information in the WHOIS would be displayed publicly, while the rest would only be accessible to those who request the information through the registrars or operators and can prove they have a legitimate reason for doing so (a court order, for example). According to this Temporary Specification, ICANN's contracted parties (registries and registrars) must continue to collect information from users who register a domain name. This proposal continues under discussion.

The following questions were presented to trigger the discussions.

The GDPR and its impact on the DNS

- What can we do to strike a balance between privacy/personal data protection on the one hand and security/operational stability on the other?
- What are the lessons learned about the impact of regulations on global aspects of the Internet?
- Can the multistakeholder model react efficiently to external events?

As mentioned in the introduction, this year, this topic has been included in the agenda of all the actors involved in the Internet ecosystem.

After being presented with these questions, the group discussed the following positions:

Johanna Falliero (academia) believes that the dichotomy between privacy and data protection vs. security is incorrect.

Enrique Chaparro (Civil Society) believes that the main issue under discussion is a contradiction. The superabundant data collected in the DNS does not support DNS stability; instead, it supports the copyright lobby. For a packet to reach a destination address it is not necessary to know the postal address. The user's physical address means nothing to the DNS function. There *is* a contradiction with the needs od law enforcement agencies. Also, the data protection lobby is against ICANN's main role.

The GDPR did not happen overnight; therefore, the fact that ICANN did not make a timely decision on the matter represents an institutional failure. There are different data storage mechanisms for large entities which, in the event of a security incident, allow taking quick action to solve the security issue. Data stored for a specific need should not cause any problem. Ultimately, there should be no contradiction between the two. ICANN is currently working on a final definition.

It was noted that ICANN considers two types of domains. Country code or generic top-level domains (ccTLDs) and generic top-level domains (gTLDs). ICANN's global policies affect gTLDs. ccTLDs have certain flexibility depending on how they are managed.

Erick Iriarte, .pr: The GDPR does not applicable in my country for two reasons. The country has its own personal data legislation passed in 2011, which is functional, as we protect the data delivered to us under the Peruvian legislation (Act 29733, Article 3, Paragraph 23). In case of cross-border services, we apply the GDPR, provided that the service is delivered directly to Europeans, and in their currency (euros). Only three types of data are currently stored: postal address, e-mail address and DNS. In his opinion, there is no standard for publishing WHOIS data.

Luis Arancibia, .cl: There are indeed cases of registry and registrars, most of which are European. There, they do have a role and are heading towards a different standard; a protection of user data.

Alberto Soto: Each government may have its own personal data protection legislation, but the problem with ICANN is that it is a global organization that must abide by the laws of the state of California and respect other legislations around the world. To process WHOIS data, numbering is all that is needed. Thereafter, it must be determined which data may be accessed freely and which must be requested through a law enforcement agency.

Other questions that came up during the debate:

What is the balance between crimes not being investigated vs. protection?

What are the minimum data needed for proper operation?

Domain name, a method for contacting the user. From an operational point of view, the problem is being able to quickly communicate with the registrant in case of technical issues or criminal activities.

What are these data?

E.C.: One possibility would be to have a point of contact, whether mediated or not. The rest of the data is for different purposes.

There is currently an ongoing lawsuit between ICANN and EPAG, which has severed its contract with ICANN. ICANN filed this legal action because EPAG recently informed ICANN that when it sells new domain name registrations it would no longer collect administrative and technical contact information, as it believes collection of that data would violate the GDPR rules. ICANN requires that information to be collected, via its contract with EPAG.

J.F.: Issues such as data security affect us here or anywhere. We should all move forward based on the same principles. Come up with standards that are for all, go beyond regionalisms. We understand that there is institutional reluctance to apply these regulations because they are more comprehensive.

To which of the principles proposed in the GDPR will we adhere? Express and tacit consent must be taken into account.

Conclusions of the debate:

Privacy vs. security: It was agreed that there is no antagonism between privacy and security, two fundamental principles that must exist and coexist. It was also agreed that it is necessary to collect only data that are relevant to their intended use, and to avoid collecting a superabundance of data, as this would be abusive. For example: a domain name holder's postal address is not necessary to guarantee the DNS function.

Participants talked about the discussions that are taking place at ICANN about the need to combine the operation of the WHOIS and application of the GDPR.

They also mentioned the differences between ccTLDs and gTLDs, as generic top-level domains have contractual obligations with ICANN and must therefore continue to collect WHOIS information, while ccTLDS vary in their form of administration and are in a more flexible position. They agreed on the importance of maintaining a point of contact with the holder, whether mediated or not. It was noted that there cannot be one WHOIS standard for all.

An update was presented on the local legislation of the countries represented in the group, and it was pointed out that, regardless of the existence of legislation on the matter, local practices had not been modified as the GDPR did not affect their territories.

Finally, it was mentioned that everyone should strive for the same principles, regardless of each country's regionalisms and peculiarities, and come up with a global definition centered around citizens; a common agreement for all, as that data should be equally protected in the region and worldwide.