Presentation by Ms Fernanda Teixeira Souza

When fighting cybercrime, we are also ensuring human rights.

For instance, my unity in São Paulo is focused on combatting Sexual Violence and Exploitation against Children online and Hate Speech online.

In the first case, the investigation and prosecution are protecting the physical and psychological integrity of the child, mainly when it leads to the rescue of the victim, but also are targeting to prevent the revictimization of the child pictured on the abuse material and also the general harm to the society, considering that the distribution of child sexual abuse material characterises incitement to the crime of sexual violence. **(UN CONVENTION ON THE RIGHTS OF THE CHILD)**

The same violation to the moral and mental integrity, harming the human being dignity, occurs in the presence of revenge porn, the online distribution of non-consented sexual material (even if the content pictured is not illegal itself), in general, with the purpose of revenge in a context of previous intimacy, although these last characteristics are not mandatory to characterize the crime. **(Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Convention of Belém do Pará)**

Hate Speech online, in Brazil, is deemed as a crime when the discourse online incites or induces prejudice or discrimination on account of race, colour, ethnicity, religion, national provenance and sexual orientation (STF ADO nº26/DF 2019), violating the right of Equality, since this discourse means that a person has less rights than another due to one of these characteristics cited. **(Convention on the Elimination of all forms of racial discrimination)**

Many many times we have seen social media profiles recruiting “candidates” to become soldiers for extremist violence. These profiles spread propaganda fomenting discrimination and trying to attract said-“combatants”.

One of these profiles was on Facebook two years before the recruiter was arrested in a counter-terrorism operation when a group that had met online was planning and had already bought armament and material to set a bomb in a Shopping Centre in Rio de Janeiro during the World Cup in Brazil in 2014.

Incitement to violence or terrorism, discrimination based on race or religion are conducts that characterize crimes in Brazil which are the limit for freedom of speech.

So, when investigating and prosecuting racism online, criminal law authorities are ensuring the Human Right of Equality which, in the balance of proportionality exam,

wins over the Human Right of Freedom of Expression, at least under some jurisdictions, as Brazil.

On the other hand, when it comes to defamation, the picture can show different outcomes:

Defamation in Brazil is a crime, but a private one. That means that the victim has herself to hire a lawyer to present a criminal query, although the police can investigate this crime if provoked.

The Prosecutor will only act if the victim is the President f the Republic or a foreign authority, under the request of the Ministry of Justice, or else if the victim is a public employee and himself requests the prosecutor taking of action.

There is one more possibility for the Prosecutor to investigate and prosecute defamation: when it is embedded in the context of elections , with election Propaganda. If there is defamation in this context, it is considered a crime to be prosecuted by a public action an the prosecutor will act.

These hypotheses, where the prosecutor can act, are directly linked to the public interest of society of knowing about the reputation and honesty of public employees, including the President. And a matter of Public State Relations, when concerning the foreign authorities.

Here again, the freedom of expression is limited by the possible harm it can cause to the personality rights that circle a person's sphere, and when investigating a defamation spread online, that has a much broader and faster reach, this cybercrime investigation is protecting the rights of the personality of someone, especially on the interest of society.

But, although ensuring human rights, many times cybercrime investigation is confronted with the challenge of not violating other Human Rights.

As we all know, the investigation and prosecution of cybercrime and other crimes committed through computer means rely on electronic evidence to be solved.

Electronic evidence can be easily altered, deleted or moved.

So, in order to Prosecutors have access to the electronic evidence in time to ensure efficacity of the procedure, some measures must be in place to grant this access.

In Brazil we have the Brazilian Civil Rights Framework, known as Marco Civil da Internet.

It statues that the companies that provide connexion/access to the internet must retain these access records for one year (MCI article 13) and that companies that provide access to internet applications must retain its records for 6 months (MCI article 15).

I am aware that data retention is a delicate matter and that the Court of Justice of European Union has annulled the directive on Data Retention 2006/24/EC in the ruling of 8 April 2014 (Digital Rights Ireland) under the argument that it entailed "a wide - ranging and particularly serious interference with the fundamental rights to the respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary".

Also, in a recent ruling ( ) the Court has decided that it would only be possible to retain data in specific and targeted cases where there is a threat of terrorism or an emergency matter. The problem here is that if a terrorist threat occurs, the investigators will need past data to discover previous steps, find the criminals and prevent the attack. In most of the cases, keeping the data onward will not be enough to prevent an attack.

In Brazil, we had this discussion with civil society at the time that Marco Civil was under national debate. It was the first bill that counted on a public platform and the contribution of all sectors of society to be written.

For us, it was a practical matter. We acknowledged the lack of capacity to have access to the data in time if it were not retained, at least, for those periods: 6 months for ISPs and 1 year for the internet connexions providers.

Unfortunately, even the steps to be taken for a demand to reach the police or the prosecutor are slow. Add to it the lack of capacity building in the matter of electronic evidence and cybercrime in a large country with different levels of jurisdiction.

We simply told the Congress we would not be able to prosecute the demands because we wouldn't have the access to the evidence in time.

Bur we really do not believe this is an interference with the right to privacy and data protection.

Firstly, companies already have and use the data to operate their business, and it is not uncommon that they retain the data for their own operations. Secondly, even before the actual Data Protection Framework in Brazil, which was mostly inspired on the GDPR, Marco Civil da Internet already had stated the obligation to the companies that held the data for the maintenance of the data, under secrecy, in a secure and controlled environment (articles 13 and 15 MCI).

In addition to it, any of this data can only be accessed under a judicial order.

So, in Brazil, IP addresses, traffic data (which includes connexion records) and content depend on a judicial order to be granted. Only subscriber information, but the IP addresses, can be obtained by the police and the prosecutors without a judicial order if they already have the concerned connexion records.

Presently, we are trying to clarify the difference between the static IP address that was used to open a profile account, for instance, from a dynamic IP address that would reveal traffic data, otherwise, everything depends on a judicial review what is not that good for the investigation, since the first step in an investigation is to acknowledge the IP address,

what has to be done very quickly, even if the data is presumably retained, because we don't know if the retention period is to be due.

So, I would like to highlight that the obligation to the companies of maintenance of the data in a secure and controlled environment, under secrecy, is already an important safeguard to the Rights of Privacy and Data Protection as it is stated on the Data Protection Regulation – GDPR, and in Convention 108. , in article 8 of the European convention for the Protection of Human Rights and Fundamental Freedoms, in the article 17 of the 1966 United Nations International Covenant on civil and Political Rights , in the article 11 of the American Convention on Human Rights

Marco Civil da Internet, as I am explaining brings most of the framework to investigate and prosecute cybercrime and crimes relying on electronic evidence combined with other rules such as the Constitution itself, the Criminal Procedural Code and other laws as the Law for interception of communication, all of them interpreted in an evolving jurisprudence.

At this point, to illustrate another challenge in safeguarding human rights when investigating cybercrime, I will bring the evolving jurisprudence concerning the access to the content of a mobile phone.

In 2007, a search and seizure order used to be very generic and everything in the targeted address could be collected, including the electronic devices, that was well accepted by the Federal Supreme Court (which is the guardian of the Constitution).

In 2016, the Superior Tribunal of Justice – STJ, which is entitled to verify if the procedures of the case where in accordance with the law, decided that even in a red-handed situation, it was necessary and specific judicial order for the law enforcement to have access to the content of a mobile phone, including data and messages exchanged. (STJ 2016 HC 51.531/REsp 1.727.266/SC, j. 05/06/2018, Min. Jorge Mussi.// STJ Dje. 09/05/2016 RHC 51.531/RO // STJ HC 372.762/MG, 5ª chamber, Dje 16/10/2017). Another important decision from the STJ at RHC nº67.379/RN, Minister Rogério Schietti that deepened the debate, took the discussions again to the Supreme Court, once the old and previous decision dated from a time when the mobile phones do not accessed internet.

The new case that was brought to the Supreme Court was about a robbery: two thieves assaulted a woman and after having knocked her down to the ground, took her purse with money, documents and mobile. When escaping, one of them left fall his own mobile phone. Police collected the mobile and accessed it immediately, getting to know the last calls the thieve had made – that had been to his girlfriend, all his contacts, and pictures, which led to his identification. He was then found innocent, because this evidence was disregarded, as poisoned , according to the Theory of the Fruits of the poisonous Tree. So, the case was brought to the Supreme Court and, after a first judgment recognising the general repercussion to the ruling, the Ministers are handing their votes on the matter, but indicating that a judicial order is mandatory in order to law enforcement to have access to the content of a mobile phone including data

referring to the record of calls, contacts, pictures and messages recorded on the phone. Not only a judicial order, but one that indicates clearly the necessity and adequacy of the measure, taking into account the principle of proportionality when balancing the right to privacy and the necessity of obtaining an electronic evidence, (Pending judgement ARE 1.042.075/24.11.17 – Min. Dias Toffoli).

Although the case law is still pending, privacy safeguards already exist in the Brazilian law:

At the Marco Civil da Internet it is clear in article 7 that intimacy and private life are protected; that the flux of communications cannot be violated but with a judicial order according to the law (the Law about Interceptions/ wiretapping (9.692/96) that states which are the crimes that can be investigated with wiretapping the voice and the written communication and the strict conditions in where it can be done; and that the stored communication also cannot be violated, unless if there is a specific judicial order.

The same parameters are used when investigating, for instance, distribution of child pornography online and the material is stored in the cloud.

In the past, an order for search and seizure at the address of the defendant, that had been identified as the point of dissemination of child pornography material, was very generic. Nowadays, the judicial order has to specify that law enforcement can search the digital devices, such as Personal computers, notebooks and mobile phones and also give an specific order to authorise the accession to content that is being held in the cloud and is reachable from the devices located in the address served with the search and seizure order.

In this situation, that pictures one of the cases of article 32 of Budapest Convention, the consent of the person who has the lawful authority to disclose the data, can be replaced by the judge's order justifying the adequacy and necessity of the measure of violating the defendant's right to privacy in view of protecting the rights of the children to not have its physical and moral integrity violated.

Fighting Cybercrime and the collection of electronic evidence pose news challenges as technology is always evolving and, as our lives are more and more digital, it is essential to put in place measures to ensure the right of privacy and to protect our data online.

That is why article 15 of the Budapest Convention sets the obligation to the Parties investigating and prosecuting cybercrime or collecting electronic evidence, when implementing the powers and procedures provided in the Convention, to have in place conditions and safeguards to ensure Human Rights as stated in many international human rights treaties.

These safeguards shall incorporate the principle of proportionality, including judicial or other independent supervision, grounds justifying application and limitation of the scope and the duration of the procedure.

As I illustrated below, a Party must have these safeguards in its national legislation in order to give the directions to being applied in a way that it is always taken into account the balance needed in the analysis of proportionality among rights.

Case law WhatsApp web wiretapping:

Right to Privacy is protected by article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, by article 17 of the 1966 United Nations International Covenant on civil and Political Rights , by article 11 of the American Convention on Human Rights, by article 7 of the Charter of Fundamental Rights of the European Union and other treaties.

The protection of personal data is stated in Convention 108 and is recognised as a fundamental right in article 8 of the Charter of Fundamental Rights of the European Union, besides having become the main scope of several instruments and legislations.

That is why the Second Additional Protocol of the Budapest Convention, which brings new instruments and procedures to facilitate the acquisition of electronic evidence, has the article 14, with 15 subsections dedicated to personal data protection safeguards.

The message here is that it is possible and a duty to fight cybercrime with the measures to ensure that human rights are being preserved and taken into account even when they have to be mitigated in order to protect other human rights that in that case emerge with superior importance.