©Dati Bendo/European Commission

Data sharing between Europol and Brazil: challenging negotiation

BY ISABELA ROSAL SANTOS (HTTPS://WWW.LAW.KULEUVEN.BE/CITIP/EN/STAFF-MEMBERS/STAFF/00155128) (@ISABELAROSAL (HTTP://TWITTER.COM/ISABELAROSAL)) - 28 NOVEMBER 2023

A new agreement for personal data sharing between Europol and Brazil is urgent. However, the need for it cannot justify not considering some crucial aspects of the Brazilian legal framework. This post highlights some topics that cannot be unnoticed during the negotiation.

On the 15th of May 2023, the Council Decision (EU) 2023/1010 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1010) was published authorising the opening of negotiations for an agreement between the European Union and the Federative Republic of Brazil on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Brazilian authorities competent for fighting serious crimes.

Negotiations with Brazil are part of the European initiative to establish agreements with different Latin American countries (Bolivia, Ecuador, Mexico, Peru (https://www.statewatch.org/news/2023/may/europol-data-deals-with-violent-police-forces-need-strong-data-protection-safeguards/)) to allow personal data sharing between Europol and international law enforcement agencies in both directions. The goal of these negotiations is to establish an international agreement to be used as a legal basis for sharing personal data to fight serious crime and terrorism, since the existing agreement between Brazil and Europol "does not cover the exchange of personal data (https://www.europol.europa.eu/cms/sites/default/files/documents/agreement_on_strategi

Reasons behind the need for this initiative include the fact that Brazil is part of the route for drug trafficking that reaches European grounds. Thus, the future agreement can have a positive impact on society, especially taking into consideration that human rights and safeguards are part of the negotiations (https://edps.europa.eu/press-publications/press-news/press-releases/2023/international-agreements-fight-crime-require-strong-data-protection-safeguards_en) on the new agreement. However, even though European Data Protection Supervisor's (EDPS) Opinion lists some recommendations for the future Agreement, other topics should be considered by both jurisdictions in the discussions for the Agreement.

The decision authorising the negotiations followed a Recommendation (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0132) from the European Commission and the Opinion 14/2023 (https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-05-03-edps-opinion-142023-negotiating-mandate-conclude-international-agreement-exchange-personal-data-between-europol-and-brazilian-law-enforcement_en#:~:text=Accept%20and%20continue-,EDPS%20Opinion%2014%2F2023 of the EDPS , issued on March and May of 2023 respectively. The Opinion is very relevant for this scenario, since it lists topics that should be addressed in the future agreement, such as the need for establishing rules for observing data principles, as storage limitation, data security, purpose limitation and data minimisation. It also highlights the need for respecting the right to information, and for ensuring safeguards such as the right to obtain human intervention in automated decisions and the need of supervision of an independent authority.

This post lists some additional remarks that require attention during the ongoing negotiations, focusing on topics related to the Brazilian legal framework on the topic.

Lack of Brazilian data protection law for law enforcement activities

In 2018, the Brazilian Data Protection Law (https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pd (LGPD – *Lei Geral de Proteção de Dados*) was approved. Similarly to the GDPR, the national law is not applied in data processing activities for public safety, national defense, national security or activities of investigation and prosecution of criminal offenses. However, differently from what was observed in Europe, Brazil has not yet approved specific regulation stating rules about processing of personal data for these purposes. This normative gap brings uncertainty to citizens and to the public authorities. Having this leverage, law enforcement authorities do not have significant obligations regarding data protection and keep non-transparent activities.

Even though there were legislative initiatives to establish a law for regulating the topic, these are still in a very initial stage. Also, since there are different regulatory actions to establish a federal law, it is still unclear which direction the future normative (also known as *LGPD* penal) will take. Thus, in scenarios related to public security, there are no rules for subjects being notified about surveillance measures and neither about possibilities regarding exercising rights (https://edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_re

Limited powers for the Brazilian Data Protection Authority

The EDPS pointed out the fact that the Brazilian Data Protection Authority (ANPD) recently became an independent body, making the data protection system in the country stronger. However, the European body did not consider that, because of the normative gap on the topic, the ANPD only has limited powers for supervising data processing activities related to law enforcement agencies. For example, legally, the Brazilian DPA can perform audits in public bodies, but it is not clear to what extend this competence applies for processing activities for the purpose of public security and fighting crimes.

Categories of data affected

Another point of attention, differently from Article 6 of the Convention 108+, the LGPD does not explicitly bring personal data relating to criminal convictions in the list of special category of personal data. By this situation, Brazil does not provide a stricter regime of protection for this category of data, what can be incompatible to the level of

protection required by parties of Convention 108+, which include the European Union.On this, another situation related to different categories of data in Brazil is that there are several legal obligations for telecommunications (https://conexis.org.br/wp-content/uploads/2022/08/Co%CC%81digo-de-Boas-Pra%CC%81ticas-de-Protec%CC%A7a%CC%830-de-Dados-para-o-Setor-de-Telecomunicac%CC%A7o%CC%83es.pdf) to retain data related to the connections made by the users. In the EU, a similar practice was considered illegal when Directive 2006/24/EC was considered invalid by the CJEU (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293), given that there were provisions that required providers to retain citizens' telecommunication data for up to two years for the purposes of preventing, investigating and prosecuting serious crimes.

Conclusion

Even though there are clear positive outcomes from establishing a specific agreement between Europol and Brazil for personal data sharing, further mitigation measures should be brought up during the negotiations. The Brazilian data protection system is recent. Although it has had substantial development in the last years (e.g., data protection becoming a fundamental right), the legal framework is still not sufficient to guarantee the data subjects' rights, especially in law enforcement activities. Thus it is crucial that these other topics are also addressed in the bilateral agreement to guarantee that other additional safeguards are put in place, guaranteeing an adequate level of personal data protection.

This publication was prepared in the context of the DARLENE project which has received funding from European Union's Horizon 2020 research and innovation programme under grant agreement No 883297.

ABOUT THE AUTHOR — ISABELA ROSAL SANTOS **@ISABELAROSAL (HTTP://TWITTER.COM/ISABELAROSAL)**
Isabela is a researcher at imec – KU Leuven – CiTiP (supervisor: Prof. Dr. Peggy Valcke) since August 2022. She holds an LL.M degree and a master's degree in Law from the University of Brasília. Her studies are focused on data protection and cybersecurity, while she's currently working at the DARLENE project.

VIEW ALL POSTS BY ISABELA ROSAL SANTOS (HTTPS://WWW.LAW.KULEUVEN.BE/CITIP/BLOG/AUTHOR/U0155128/)

TAGGED AS: DATA SHARING (HTTPS://WWW.LAW.KULEUVEN.BE/CITIP/BLOG/TAG/DATA-SHARING/), FEATURED (HTTPS://WWW.LAW.KULEUVEN.BE/CITIP/BLOG/TAG/FEATURED/), INTERNATIONAL DATA TRANSFERS (HTTPS://WWW.LAW.KULEUVEN.BE/CITIP/BLOG/TAG/INTERNATIONAL-DATA-TRANSFERS/), LAW ENFORCEMENT