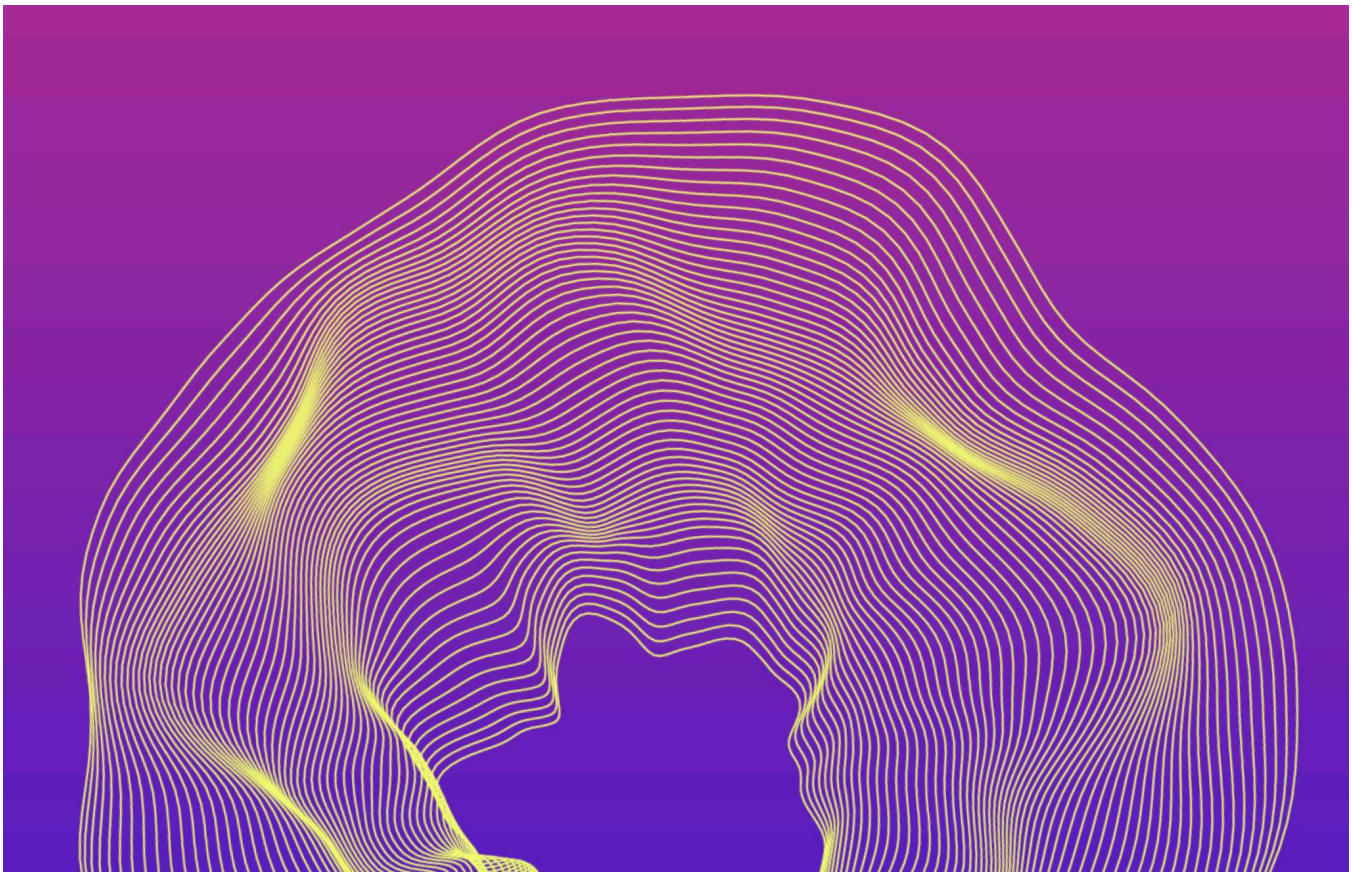
Exceptions to Data Protection Regulations: Lessons from the Data Privacy Learning Series

Data Privacy Brazil • Apr 6, 2022 • Uncategorized



When discussing data protection regulations, particularly the passage of comprehensive data protection laws, the issue of what falls within scope and what exemptions exist to circumvent them often arises. This comes into focus in reviewing the cases in which personal data processing for the purposes of public security, national defense or criminal persecution are weakened or completely excluded from the application of protective legal frameworks.

This is not news. A supposed trade-off between countering criminal activities on one side, and upholding the privacy of citizens on the other, has always been at the center of legal debates and often resulted in different degrees of compromise in fields such as telecommunications, counterterrorism and criminal procedure in order to allow for the use of personal information for these purposes.

With the advent of new technologies that allow for more intensive data processing, individual and group profiling and ubiquitous data surveillance, data protection regulation is also faced with the challenge of safeguarding against abuses and disproportionate employment of their personal data for otherwise legitimate purposes.

This is a reality currently faced in Brazil, for example, where a general data protection law that exempts these activities was passed in 2018.This kind of formal exemption to the standard protections afforded by the broader law are the cause for growing concerns with the use of facial recognition technologies by police and predictive policing. Similar discussions are being held in other countries in both Latin America and Africa, including those who have not yet a comprehensive data protection legislation but have analogous experiences in other domains.

With that in mind, the second workshop of the *Data Privacy Learning Series* – took place on January 13th, 2022 and with a focus on **exemptions to privacy and data protection regulations for public security, national defense, criminal prosecution, and related matters**.

The meeting started with three brief presentations by partners, who presented specific cases and experiences to set the stage for an open discussion to discuss the issue across different contexts. These presentations focused on automated facial recognition technologies in Brazil and the current legal battles the country faces and on spy tools/other examples of direct surveillance in Nigeria and Ethiopia.

The main goals for this second workshop were:

- To discuss, based on concrete examples, the problem of exemptions to data protection legislation (or other cases where the law does not apply) for purposes of public security, national defense and criminal persecution, as well as the potential insufficiency of existing legal mechanisms in the face of more complex and

intensive data processing, profiling and automation of decision-making in these areas;
- To build collective insights into strategies to deal with this problem, such as exploring data protection principles and constitutional provisions on privacy, due process and other safeguards in the face of these phenomena.

Brazil: automated technologies of facial recognition vs the current legal landscape

As a way to contextualize and situate the discussion, a brief overview of the many concerns around the use of facial recognition for purposes of identification and surveillance was presented by Coding Rights, building on concrete examples of how the structural racism embedded into these systems has already resulted in wrongful arrests in Brazil.

This discussion also raised other high profile incidents, such as when actor Michael B Jordan, who isblack, appeared on a wanted list from the Civil Police of a Brazilian state after being included in the "photographic recognition catalog" used in their law enforcement operations. The absurdity of this example shines a light on a practice that is becoming increasingly widespread in Brazil, to the point that the Brazilian National Justice Council was pressured into creating a working group to regulate it.

Meanwhile, Brazil has successfully passed both a digital rights law and a comprehensive data protection law and has also included data protection as an autonomous fundamental right in its Constitution. The processing of personal data for purposes of public security, national defense and criminal persecution, however, lacks precise regulation, despite the best efforts of a Commision of jurists to draft one, with continuous support from civil society organizations and activists. Considering this scenario, and the growing use of automated technology in policing in a country where structural institutional racism is the norm, civil society is working on alternative strategies to protect people's data, but also other fundamental rights, such as non-discrimination, freedom of expression, assembly and association, bodily autonomy and even the right to life.

One avenue to address these exceptions that partners discussed during the session centered on directing efforts to ensure the protection of personal data in other pieces of legislation that are being discussed and also have a strong impact on areas that are currently exempted: examples are the New Criminal Procedures Code and the adoption of the Budapest Convention by Brazil. Another approach that was introduced to overcome the obstacles posed by a lack of specific regulation and the fact that Brazil is moving towards a generic ethics-based approach towards AI has been to focus advocacy

efforts at the municipal and state level to push for local laws that prohibit the use of facial recognition technologies by the State.

Nigeria: An emerging surveillance State left unchecked

Currently, Nigeria has in place some regulations on data protection and related matters, such as the subsidiary Nigeria Data Protection Regulation (NDPR) from 2019. However, there is no comprehensive and exclusive statute governing data protection in the country at this time. Laws that allow for State surveillance, on the other hand, have existed for decades, particularly related to criminal persecution and matters of national defense. The scenario in the country regarding the use, and possible abuse of personal information by State agencies is of one opacity and uncertainty.

The scope of application for the NDPR (Nigerian Data Protection Regulation) is limited such that State activities that involve data processing, in general, are mostly not covered. Besides, while there are indications of surveillance being conducted in a widespread and abusive manner – for political goals, for example – the subject is essentially a black box, which makes it hard for civil society and activists to differentiate between what's a structured State authoritarian use of personal information and what's the product of corruption within the government.

Furthermore, a general public distrust towards the State doesn't necessarily lead to more engagement and a push for data protection legislation that has jurisdiction over State activities. While data processing by private companies is largely seen as needing regulation and enforcement, issues of insecurity and insurgency (and the corresponding "trade-off" with privacy and data protection) are harder to counter. In that sense, data protection advocates in Nigeria face a double challenge: to push for stronger data protection in general, while also focusing on State activities that remain largely out of the scope of both existing and proposed regulation.

Ethiopia: it's not just the government

Ethiopia shares a similar context as Nigeria in terms of the ubiquity of physical and digital surveillance by governments legitimized by several legal provisions in the areas of criminal investigation, national defense, counterterrorism, fraud investigations and financial matters, in general. Unlike Nigeria, however, Ethiopia does not have any non-constitutional provision on data protection: while the Constitution itself provides for privacy and personal data protection, specifics must be determined by ordinary legislation. There is a zero draft data protection law – which itself provides broad

exceptions for the public sector – but no substantial advances have been made yet on that front.

Two other trends can be highlighted from Ethiopia's current situation, which other Southern countries strongly relate to: one is the introduction of a National ID system in the country, which tends to boost the state's surveillance capabilities, including by centralizing existing databases without a corresponding data protection framework. The second is the role played by private actors, particularly after 2018 with the emergence of social media and tech companies presence in Ethiopia: meaning that the monopoly that state actors held over the use of surveillance was overrun and organizations and activists have also become more concerned with lack of accountability by private companies.

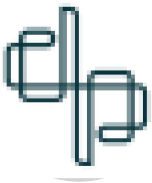
Collective learnings and open questions

It was possible to observe that not all ADAPT partner countries share the exact same priorities when it comes to exemptions from data protection provisions. While Ethiopia and Nigeria are increasingly more concerned with direct surveillance practices by their governments coupled with a lack of specific legislation, for example, Ecuador and Bolivia express more significant concerns about the flexibilization of data protection norms enjoyed by the financial sector. When it comes to intensive use of personal data, including through automated technologies, by public security agencies and legal strategies to counter these practices through specific data protection provisions, Brazil brings some interesting strategies to the table, such as municipal and state level advocacy.

As a general takeaway, the workshop showed how the successful enactment of general data protection laws does not necessarily take away from the challenge of regulating personal data use by the public sector, particularly in areas that are considered "sensitive" and have traditionally enjoyed broader access to private information. Having well-established and wide reaching provisions is a necessary step, however, for two reasons. On one hand, the efforts to pass comprehensive data protection legislation tend to bring together a wide range of stakeholders, including those that otherwise have competing interests, as well as shedding light on the issue as a whole and allowing for it to break into mainstream debate. On the other hand, it may be an opportunity to actually discuss specific legal parameters for these activities in light of a new found concern about the abuse of people's personal data through digital means.

Open questions from the workshop remain and must continue to be addressed in multistakeholder and diverse forums, focused on Global South particularities. Some of them are:

- In less-than-ideal circumstances to pass any data protection regulation, how should activists handle the need to engage public officials versus concerns with certain immunities enjoyed by these same actors? What are concrete examples of these "trade-offs" both during the lawmaking process and after the enactment of legislation?
- What are concrete successful strategies to engage other stakeholders – such as the private sector and the general public – to the importance of also regulating personal data use by public agencies and counter the prevailing narratives of security and stability over privacy?
- How to navigate scenarios where the adoption of more advanced data-driven technology can indeed be a tool for dealing with structural problems in Global South countries, including in areas such as intelligence and public security, but is also likely to deepen existing asymmetries of power and information and discriminatory practices?



Data Privacy Brazil

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

direct

© 2023 · **Direct** · All rights reserved

Blog at WordPress.com.