noesis
an Altia Company

Data Protection & Privacy: How organizations can Protect and Innovate with Data

With the democratization of the use of Artificial Intelligence and the implementation of Machine Learning models, more and more volumes of sensitive data are managed by Organizations. This large volume of critical information is inherently a desirable target for cyber attacks.

If "data is the new oil," as The Economist stated in 2017, it is essential to adopt a strategy to protect such an important asset.

Thus, the topic of Data Protection and Privacy should be at the center of the concerns and priorities of any manager, especially the CIOs of organizations.

Indeed, **according to Gartner, it is estimated that as of 2022, 30% of attacks will focus on data that are the source of machine learning models**.

Although it is noted that organizations are increasingly aware of this issue, concerned with improving their internal processes, this is a critical issue, with a tendency to increase in the coming years. Cyber attacks will become more and more frequent and more sophisticated.

Contrary to what you might think, and even if they assume they are more vulnerable, this is not an issue that only affects small and medium-sized companies. Also, large organizations with the most sophisticated security systems have seen their data and their security systems AI being targets of attack, as were the cases of some technological giants and global companies.

Thus, for the implementation of a Data Protection strategy, it is necessary, on the one hand, to increase the awareness of the business fabric for this theme, but also to increase its technical know-how, essentially to identify where to innovate without compromising the data security.

WHAT CAN COMPANIES DO TO LEAP?

Companies must realize that their customers will be increasingly loyal to organizations that ensure security and privacy. Data security must therefore be a pillar of your activity. Innovatively, a company that wants to create different services and products fostered by data solutions, artificial intelligence, or analytics must ensure the necessary tools to protect this data and define proper data protection & privacy strategy.

One of the possible solutions is for the data to be "pseudo-anonymized." If an operational database is protected, when it is migrated to the Cloud, it must be subject to an anonymization process. Thus, in case of a cyberattack that manages to overcome the various layers of the organization's security and access the database, the information collected will not be relevant. It will not be possible to identify people or relate this data with individuals. Using this strategy, the data that is encrypted and not the database is the data that will always be protected.

Therefore, the leaders of organizations must look at security at the level of their networks, infrastructure, or peripherals and in a whole perspective of preventing attacks. It is also necessary to think about security in case of a practical perimeter breach, ensuring that access to data, if compromised, will have no consequences. It will not be possible to extract readable information from these data.

This data protection strategy thus works as a last layer of defense in organizations: an innovative approach and an added layer of security for anyone working with data.

By correctly adopting this "pseudo-anonymization" strategy, sensitive information is consistently protected, allowing specialists to aggregate and work with it, resulting in effective innovation processes, always in a secure manner.

With the growing adoption of artificial intelligence on a scale, this will be the big challenge for the time being – ensuring that organizations' security and privacy teams are alert to data protection and have the tools and know-how necessary to implement Data Protection policies.

THE IMPACT OF ANONYMIZATION ON DATA SCIENCE AND DATA PROJECTS.

In addition to this awareness among the organizations' security teams, also at the level of data scientists and engineers, it will be necessary to invest in specific training. The privacy of information is not restricted to the pseudo anonymization mentioned above. It may also require anonymization. It becomes essential to understand what identification risk means. In organizations where a data structure already exists, it mustn't be based only on direct indicators (name, age, social security number) but on several indirect hands (age, salary, for example).

Anonymization aims to minimize the risk of data identification based on indirect factors.

On the other hand, in addition to the technical issue of data protection, there is also the ethical plan, which will have to be increasingly emphasized in the activity of any Data Scientist.

CHALLENGES FOR THE FUTURE

In the USA, we are already witnessing a growing adherence of Companies, for example, in the insurance sector, to the theme of anonymization, greatly enhanced by the legislative changes introduced, namely with the IPA (Investigatory Powers Act) legislation. As for Europe, there is a significant disparity between how the various countries approach this issue, with some concern regarding the adoption of Data Protection policies, by public and governmental entities and concerning citizens' data concerns.

THE PORTUGUESE CASE

In Portugal, the big challenge is trust. It is necessary that organizations have a plan for this topic and, at the same time, that the fear of possible attacks does not affect their innovation strategies and bet on data. Innovation will necessarily go through the scaled adoption of Artificial Intelligence and, for that, migration to the Cloud is inevitable. This unavoidable movement forces organizations to be ever more attentive and awake to the Data Protection theme.

One of the main competitive advantages for organizations will be adopting a data protection and privacy strategy.

5 STEPS WHERE WE SHOULD START:

- Identify the security, privacy, and data team;
- Identification of the common problem
- Define a roadmap for the strategy, using partners specialized in the theme
- Adopt the appropriate technology specifically focused on Data Protection
- Implement the strategy

From the CEO to data science, this is a mission where everyone has a role to play, namely when it comes to exposure and attention to these themes. Only in this way will it be possible for us to be more secure and guarantee the privacy of the data entrusted to us!

ABOUT PROTEGRITY

Protegrity protects the world's most sensitive data wherever it resides. Our industry-leading solutions allow businesses to finally tap into the value of their data and accelerate digital transformation timelines – without jeopardizing individuals' fundamental right to privacy.

noesis
an Altia Company

Noesis is an international tech consulting company offering services and solutions to support clients in digital transformation and the development of their businesses In order to obtain sustained value that is transversal to all sectors. Noesis is focused on infrastructures, software, quality and people. The organization is based on highly specialized talents, operating in nine business units and six countries Portugal, Spain, the Netherlands, Brazil, Ireland, and the USA. Since 2020 Noesis has joined Altia, listed on The Alternative Equity Market. With this incorporation, Noesis is now part of an organization with more than 2000 employees, 3 Datacenters and 20 offices.

noesis

an Altia Company