# Experts looks at how AI is influencing data protection in apps

*We live in a world where the fact that businesses collect user information for marketing purposes is no longer frightening to anyone. Yes, we’ve taken specific steps to prevent massive misuse of personal data. However, we’ve all made peace with the fact that our personal information is wandering around the enormous clouds of tech giants.*

Temps de lecture : minute

*25 October 2023*

The data protection issue is gaining new acclaim as AI imminently enters our lives. For tech products, integrating AI into their mobile apps becomes a matter of competition – if you do not somehow make AI a part of your app – you’re doomed to lag behind the market.

But as the legal regulation is vague on AI and data protection issues – should we take new measures in this direction?

We’ve turned to experts and opinion leaders for their versatile takes on data privacy in the AI-driven world.

## AI Rush vs Reason

AI integration has become a life-and-death matter for many businesses. Rightfully so, any downturn in applying AI can kick your app out of the race for many years ahead.

This AI rush reminds me of when we did not know much about the pandemic and the cost of living crisis. That was when startups were mushrooming under the rains of lavish investments. Back then, many co-founders thought that having a five-star idea was all it takes to build a successful product. And it was true to some point – investors would generously give you the money once you charm them with another idea that “*would make the world a better place.”*

Yet, soon enough, we saw a parade of startup failures, like *Segway*, *Google Glass* and *Juicero*, which had one thing in common – their idea did not solve any real user problem.

We can see the same with the AI hype-wagon – some businesses rush to make it a part of their system but rarely think of what value it brings to users. This is what *Soren Nielsen*, *Thursday Consulting*, former fintech entrepreneur and author of the book *Death by Innovation Theater*, thinks of this massive interest.

“I’ve seen many fintechs fall in love with technology, and right now I meet many wanting to just do ‘something with AI.’  That's not enough. AI should only be used if it solves the problem of the users. If it does it should be used the same way as the GDPR regulation works – by only capturing the necessary data of the users. Both the use of AI and the data shared with this technology has to have a purpose.”

# How to Ensure Data Privacy in AI-Based Apps

Firstly, this is a mix of measures at different levels – regulatory, technical and educational.

“Data is the lifeblood not only of every organization, but also of every single Customer or Person. When AI is core, we have to ensure not only a protection directly connected to App usage, but also, we have to prevent a misuse of personal and sensible data on a different scale that involves how those data could be used to “discriminate” or enforce biases and discrimination, i.e., to limit access other financial services,”  says *Roberta Robin Gilardi*, CEO and founder of *G-Gravity*.

Since AI is intensively entering our lives, the data privacy issue is becoming more challenging and raises data protection issues again. With AI, data collection can go uncontrolled, resulting in massive information leaks and manipulations.

Yet, the importance of inventing new data protection measures in AI can hardly be stressed enough, especially in sensitive domains such as healthcare and fintech.

“In the ever-evolving landscape of AI-powered finance, the protection of user data isn’t a mere obligation; it’s our defining mission. Just as a sturdy vault protects precious treasures, robust security measures must shield the financial well-being of the users.”, – *Yan Likarenko*, Project Manager at *Uptech Software Development Company*.

While the regulatory bodies are struggling to decide how to put the AI vs. data issue in legal frames, the burden of responsibility has fallen onto the shoulders of developers. And regulatory bodies do not mind!

For one, the UK’s data protection watchdog has clarified its expectations in its *latest warning* – AI app developers should cover all privacy risks before bringing AI-powered products to the market.

“The whole AI vs data privacy issue is rather vague, rather than certain. As for legal regulation, there are no specific acts covering how data should be protected in the world of AI. So the significant part of responsibility here falls onto the shoulders of developers.

Yet, not everything is clear here as well. There are usually two scenarios by which developers can integrate AI into the app – via API integration or building a customized AI model. In both cases, there are not clear ways to fully encrypt personal data in processing, yet, there are certain ways to make it more data-ethica,"  says *Andrii Bas*, CEO at Uptech Product Studio and *DYVO*.

## Homomorphic Encryption as a Theoretical Solution

Imagine if you could put your data into an envelope, send it, and the receiver would be able to read your message even without opening the envelope – sounds like a fairytale? Well, this is pretty much what "Homomorphic Encryption" is about – the magic of math in action!

The homomorphic encryption technology is widely discussed in financial circles as an effective instrument that could provide data processing and exchange between banks and financial institutions.

"Homomorphic encryption has plenty more potential applications in the financial world. By securely sharing and analyzing data, institutions may be able to clamp down on credit card fraud (by, for example, sharing information about fraudulent activity with other banks), and better manage risks associated with loans and mortgages. Customers are also more likely to trust a bank if they can be assured that their data is being encrypted using the highest security techniques," says *Romain Servant*, Financial Expert and Startup Advisor, Presales Solution Manager at *Ingenico*.

While discovered long ago, homomorphic encryption gained traction among financial specialists only in 2009, when Craig Gentry, a Ph.D. student at Stanford University, claimed it is theoretically possible to process encrypted information without decrypting it.

While the whole idea looks beautiful and somewhat mysterious, its practical usage is still open to question. The main hurdle that keeps homomorphic encryption from becoming a subject of common usage is technical and legal.

The technical hurdle is the extremely low speed of the technique. Romain Servant comments on that:

> *“Today, the fastest homomorphic encryption tools are around 1,000 times slower than using unencrypted data, but that difference will continue to drop.”*

The advent of AI in our lives and apps is creating a new wave of discussion about data protection. Though there is still big uncertainty about how to treat data in AI-driven apps, one thing is clear: action is required at several levels: legal, technical, and educational.

Dima Kovalenko is co-founder and CEO of *Uptech Software Development Team* and *Rozmova*.

---

Article écrit par Dima Kovalenko