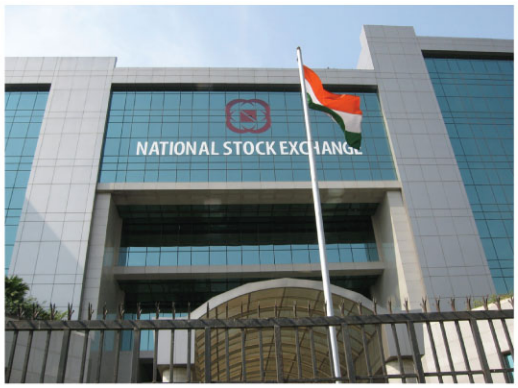
Analytics India MAGAZINE

Data Paradox: Privacy Laws Will Soon Be Applied In India. Here's What It Means In Data Analytics

KSHITIJ JAIN JAN 21, 2019



In 2018, the much publicised Facebook and Cambridge Analytica news brought to light a very important aspect of our digital existence: the consequences of data misuse. Most importantly, it served as a catalyst to get people thinking about their digital footprint and how they want companies to treat their personal data. It was an impending disaster that required lawmakers' attention, and it also catapulted a wave of personal data protection regulations being drafted across the globe. The European Union's General Data Protection Regulation (GDPR) set the bar really high and was a wake-up call for everybody impacted by technology. For India, the Personal Data protection bill, too, has been garnering attention due to its far-reaching impact on data privacy and security.

Coming to think of it, these privacy regulations will be most challenging for data scientists as it will push data usage in precisely the opposite direction to where it was intended to lead in the first place. Data analytics is about drawing unanticipated insights from what was thought to be innocent data, which is why, Data Science goes about acquiring new data and finding new uses for existing data. On the other hand, privacy laws advocate minimal data collection and restricted use of personal data, whether digital or traditional. The impact for data scientists includes the ability to collect, use and transfer data. It (would) require consent for access to end users' terminal devices like phones, tablets, wearable gadgets, etc to collect metadata. While first-party cookies can be used for analytics, it would impose severe restrictions on the use of third-party cookies. This means, metadata usage will then be limited to statistical counting, and would be required to be deleted immediately after the function it was collected for is complete.

Consumer Is The Ultimate King!

These laws go to show who the real boss is. The thing is, consumers' concerns about how their data is used and shared are valid and has long deserved lawmakers' attention because the volume and complexity of digital data are increasing exponentially. In the near future, data privacy will be seen as a civil right with greater emphasis on control and consent on how their data is used. They could even have the right to opt-out of automatic profiling algorithms, however, this could produce additional bias – but then that's a different debate.

The Other Side

So what does this mean then for small businesses that rely heavily on targeted advertising tools, cloud-based software and digital marketing automation tools in order to grow and increase profits? That's because digital marketing tools like targeted Google and Facebook ads to reach potential new customers rely heavily on services in the Cloud to manage and store customer data. In its very format, laws like GDPR establish strict guidelines for securing a user's consent before advertisers can target them; and restricts the access and use of first-party data. This leaves the advertiser completely visionless when it comes to consumer preferences. Chances are, with laws and heavy penalties, data entities could make those tools less affordable, less effective and more difficult. A balance must be met between the needs of both – consumers and businesses. While the initial fear of losing out on customers due to GDPR may have subsided as we see the ad-tech industry being active these past months.

Drawing A Balance

Along with ensuring that data is only collected for a specific purpose, GDPR also stipulates that user information should only be stored in the minimum number of locations absolutely necessary. The trouble is that businesses often do not know themselves where, and how much, user data is being stored, where it is replicated, and what the risks and privacy implications of that data may be. The security features of many cloud storage systems aren't foolproof enough.

Tables Turned

It has been more than six months since the GDPR was implemented. It has indeed changed the way we think about security, compliance, and consumer consent. It has for a fact changed data collection, sharing, and transfer and yet, more recently, in September, the Facebook engineering team discovered a security issue affecting almost 50 million accounts. What does it really say about data security anyway?

Having said that, digital analytics would need to have safer and transparent data compilation and work to ensure consumer data privacy. The inability to adhere to laws will lead to stiff regulatory fines and this will certainly produce an environment where corporations are very reluctant to buy, sell or share data that may be personal. Perhaps, it also calls for a shift in the content strategy of the learning industry as well. Emphasis must be given to adapting ethical practices and on finding fitting ways to use data, bearing in mind the global privacy laws. In the Data Analytics programs offered by NIIT, we sensitize students about these ethical issues. Because, in the end, compliance is the key and responsible data collection and usage will be the only way forward to survive in the extremely competent digital economy.

https://www.analyticsindiamag.com/data-paradox-privacy-laws-will-soon-be-applied-in-india-heres-what-it-means-in-data-analytics/