Data Protection and Privacy in Europe and United States: What You Need to Know

by Boran Göher

The discourse regarding the safety and privacy of personal data in digital mediums has always been present on the internet, but due to a combination of increasing use and variety of social media platforms and the accelerating merge of real and online personalities, the topic is now livelier than ever. Indeed, in the older days of the internet, people spent much less time on applications and websites that stored data, and what time they had spent was mostly under an alias. Now that the trends have changed for the opposite, the topic of data safety is very much in the spotlight. And when this topic is being discussed, you will notice that people will often preface their statements with where they live. This is more or less a necessity in today's world, where different countries have wildly different laws on the subject. Yet it complicates things for the onlookers, as they have to be familiar with each country's law to understand the debate. This article will aim to introduce our readers to the two most important legs of this discussion, so as to give you the necessary context to enter the world of digital data protection laws, these legs are the laws in the EU and in the US.

First of all, let us start with the main difference, and the main reason that comparing the two legal systems is difficult. The EU, always a more centralization supporting organization than the United States, has one main element governing their data protection laws. The GDPR is the main article of the EU on data protection, and it controls every aspect of the EU's data protection laws. There is no direct counterpart in the USA, however, the data protection laws in the States are mostly specific to the sector they apply to. There still exist various acts that provide general governance, but they are industry-specific like the HIPAA and the GLBA. (1)

The second biggest divide between the systems is how they approach the issue of privacy. In Europe, data privacy is discussed alongside data protection, and the laws also reflect that. It is to be expected, after all, those are both protected under the EU charter, so the GDPR has to

tackle them both. In the US, privacy is a whole different hassle from data protection, so the two do not get mixed up much in the legal side of the business, if it is not necessary. Returning to our original point of following a discussion on these laws, you might have noticed that people from the EU are much likelier to talk about how the introduction of new laws has impacted corporate operations in their country. While not exactly draconian, the EU does follow through on their legislations more zealously than the US, caused in part by the structural difference between the laws and partly by the less forgiving nature of the EU towards corporations. If you follow the news, you might also remember many big digital firms changing their digital data policies to suit EU laws a few years back. The law in this case, and at the beginning of this paragraph, is the GDPR, and it brought along a great deal of change with regards to data protection and privacy.

Well, all those points really do tell us a lot about the differences between the US and the EU, but they mostly pertain to the form of these laws and not the function. To complete the picture, we have to consider what they do differently as well, along with how it affects the end outcome.

Let us start with the GDPR. The GDPR is committed to protecting a few key pieces of data. These key pieces of data include but are not limited to, sexual orientation, racial/ethnic background, biometric data, and address and ID numbers. (2) And the laws protect all this information with the same importance. In more specific terms, all these must be “reasonably” safe, or so the GDPR says. American law would also tell firms to protect all this information, but you can be sure that Social Security Numbers will be much more well-protected than, say, sexuality information. This is sometimes expressed as ease of business for firms in America, but that is an optimistic spin of things and might be a sign that American laws are not strict enough.

We had previously mentioned that privacy was developed separately from the main branch of data laws in the United States. Separately here means that most privacy laws are enacted on a state level since privacy laws at the federal level are almost nonexistent. This does not mean that the state laws are not close to nonexistent though. Even in the current year, Very few states recognize privacy as a right, and therefore the legislative process is not often fruitful for satisfying privacy laws. Compared to Europe, the privacy side of the matter is in shambles in the United States.

By all this information, what do we make of the overall situation, or rather, what should we make of it? From our analysis, it seems that American laws are a bit behind on the issue compared to Europe, but I do not think that it would be fair to say that this is the finalized form of the situation. The issue is still young, compared to other things regulated by law, and we may regard America's incomplete laws as room for growth. Do I actually think that data protection and privacy laws in America will eventually be better than those in Europe? Definitely not. Yet, it is best to keep an open mind if you wish to understand this issue.