It is not the first time cyberspace becomes the battleground for debate, argument or even war, but when Artificial Intelligence (AI) meets personal privacy, the stakes may never have been higher.

Ida Thorsrud, a lawyer specializing in European privacy law explains that what we are now seeing may change power dynamics between governments, citizens and corporations for the foreseeable future if not dealt with responsibly.

* The biggest problem from where I’m standing is how easy it would be for us as humans to use AI in decision-making, rather than as a tool to help us make informed decisions ourselves.

(faktaboks om GDPR:

GDPR (General Data Protection Regulation) is a set of European Union regulations that govern the collection, processing, and protection of personal data.

)

While GDPR does limit automated actions, such as deciding whether or not you get a mortgage or insurance, or more crucially, what kind of healthcare you will be provided, there will always be those who try to bend the rules. According to Thorsrud, several Norwegian schoolkids are currently in conflict with teaching staff after teachers asked ChatGPT whether their submitted work was original. However, finding out whether or not something has been created by generative AI is not something generative AI itself is capable of.

* Generative AI is not a fact-machine, it merely gives you the most probable answer, based on the data it has been trained on.

In her 2023 book, Inga Strümke poses the following scenario: A self-driving car is driving along the road, but due since we as humans tend to become quite laid-back when processes are automated, the driver is not able to react in time to avoid hitting the pedestrian in front of it.

As a visceral example, the self-driving car hitting an unwitting person is easily understood. But what happens when the automation takes place in cyberspace? Thorsrud worries about that complacency may spread further, and eventually reach her own field of work: The Law.

Harald Husum is a machine learning engineer at the Norwegian data science firm Intelecy. He explains that while machines are great at crunching numbers, they have their limitations.

* No machine learning algorithm is useful without good data. And it is worth noting that while we call it “generative artificial intelligence”, it is more generative than intelligent.

(faktaboks om jurisprudence:

Jurisprudence establishes the basis for future legal decisions by setting principles and guidelines for interpreting laws, often based on higher court rulings.

)

What could happen if, as Thorsrud worries, our legal system becomes automated in the name of efficiency and public spending? Certainly, any historical inequality or discrimination will be far harder to combat with an increasing belief in society that machines cannot and will not lie. What the experts advise is caution and reflection, not delving into Luddism.

Nearly every business and organization that handles personal data to any extent is required by GDPR to keep processing records for what they store. In addition, any citizen in an EU/EEA country should have access to their own processing record. Certainly that could be automated, and it already has. Making personal records readily available for private citizens not only benefits them, but also businesses that no longer need staff to manually process requests for access.

As AI technologies are advancing at a breakneck pace, privacy laws are struggling to keep up – with EU being the flag-bearer for those who wish to keep personal integrity part of the conversation. In between promises of more efficiency, more captivating entertainment and cheaper goods, it’s hard for individuals and small and big business alike to put a price tag on our personal data.

Not only will AI help tech giants, governments and the PR industry tailor their systems to meet our needs and wants – these AI algorithms require a huge amount of data to reach a level of efficiency where they can be useful.

We have just seen the beginning of automation, and these systems are incredibly hungry for more data.  
- Harald Husum”

In 2013, long before the implementation of GDPR, the Austrian lawyer Max Schrems, filed a complaint against Facebook, claiming they broke pre-GDPR European privacy laws when transferring his personal data from Europe to the United States. Such data transfer required strict protection. Also in 2013, the revelations brought to light by former Edward Snowden made the nature of such protection questionable. It was clear from the leaked documents provided by the ex-NSA contractor that extensive collaboration was taking place between US intelligence agencies and social media companies.

Since the ruling that suspended data transfer to the US and other third countries, in what is known as Schrems I in 2015, Schrems has continued his work. In 2017 he founded the non-profit NOYB, short for None Of Your Business, and later took Facebook to court once more.

There haven’t yet been landmark cases with the same level of jurisprudence provided by Schrems II and II, but several data regulation authorities in the EU have dealt with cases concerning automated decisions.

* We will soon get a ruling on automated mortgage applications

Ida Thorsrud

In the highly digitized countries in the EU, the impacts of the Covid-19 pandemic were certainly felt in schools, the workplace and social settings, other areas of the world were far more severely impacted. Technological advances have a tendency to impact certain industries and job markets in very different ways.

* The factories we are helping become more efficient still have workers in them, but I see how automation can impact both job opportunities and individual privacy if not applied based on a moral framework.

Harald Husum, machine learning engineer

Other parts of the world also have far weaker privacy regulations. While any company that wants to do business with European customers are required to follow EU regulations like GDPR, there are ways to still put domestic citizens under surveillance. In 2021 Washington Post reported (https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/) that the telecommunications company Huawei is heavily linked to the Chinese Communist Party’s surveillance programs.

Some of these programs are targeted at minorities like the Muslim Uyghurs in Northwestern China. Others apply scores to individuals, measuring their social cohesion and public behavior, cracking down on things like jaywalking and intoxication. According to the same Washington Post article, IBM and other tech companies made the conscious decision not to sell their facial recognition software to law enforcement due to fear of unethical and otherwise inappropriate applications.

Privacy has been challenged by government and businesses in various degrees throughout history. Still, the introduction of global mass communication in the last decades now paired with the ability to parse enormous amounts of data in fractions of a second worries the experts.

The EU’s ability to implement and enforce a global standard for privacy is closely tied to its market power. While the EU remains an economic super-power today, PWC projects its combined share of the world economy could fall below 10% by 2050, with the United States also falling compared to emerging economies like India and Indonesia. (https://www.pwc.com/gx/en/research-insights/economy/the-world-in-2050.html)

* Individuals will simply have to be more educated, more aware and take more responsibility for their own privacy and cyber risk mitigation.  
  August Aunan, security engineer, Norwegian Police IT Unit

Enforcing a solid framework like GDPR is only half the job, as long as companies and criminals make it easier to share personal data than not. Husum hightlights the importance of educating not just IT professionals, but the general public.

* Not everyone needs to understand the algorithms, but if everyone from schoolkids to grandparents had a more solid understanding of *how* they work. From filter bubbles in social media to advertising trackers, our resilience in a world that can be quite enchanting requires one simple thing: Knowledge.  
  Harald Husum, machine learning engineer

As we continue to navigate the complexities of AI in a global context, the importance of balancing technological advances with ethical considerations seem to be top-of-mind for the professionals. While legal frameworks like GDPR are critical in ensuring civil rights in today’s digital world, cooperation, knowledge and ethical considerations of individual governments and businesses may be equally important in securing a future free from corporate and government surveillance.