Sociology and Social Work Review Volume 6 (Issue 2)/2022 | pp. 93-101

DOI: 10.58179/SSWR6208

https://globalresearchpublishing.com/sswr/

Government surveillance and facial recognition system in the context of modern technologies and security challenges

Gianmarco Cifaldi[a*]

[a] *University "G. d'Annunzio" of Chieti-Pescara, Italy*

Abstract

The challenges to privacy resulting from the use of modern and constantly improving data processing technologies pose a significant threat not only at the personal level, but also at the national level. The proliferation of biometric systems, and specifically facial recognition technologies in our everyday lives, has prompted the need to foster a public discussion regarding the associated societal and ethical concerns. Modern information and communication technologies allow organizations to process data on an extremely large scale and at an increasing speed. This thesis is reaffirmed by the exceptional economic strength of companies that process and store personal data on a worldwide scale (Alphabet, also known as Google or Meta, the company that owns Facebook and Instagram), or by the recent acknowledgment of this issue by several countries and the European Union. This paper highlights the state-of-the-art in data processing technology and centers on the numerous difficulties in handling data. It focuses on ethical, technical and legal concerns regarding facial recognition systems and also emphasizes the technologies available and their capacity for handling the larger volume and variety of personal data processing and Big Data Analytics.

Keywords: *facial recognition; government surveillance; big data analytics; artificial intelligence; security challenges; machine learning.*

1. Introduction to data processing

The World Wide Web has made communication in many areas of life so quick and easy that in some cases one might think it has eliminated the need for national borders. The internet can become the center of a person's everyday reality. On the internet, it is quite simple to find work and make money, socialize, learn, educate oneself, entertain oneself, and shop, leaving online traces of one's personal information while doing so (Altieri and Cifaldi 2018). Due to how much it now dictates how businesses connect with their consumers and how it positively impacts customer experience, personal data has

[*]Corresponding author: Gianmarco Cifaldi, *E-mail: cifaldi@unicht.it*.

become valuable to the point where it is referred to as "the world's most precious resource" ahead of oil (The Economist 2017).

In the highly competitive industry, proper and effective development and use of contemporary technologies are essential. Blockchain, artificial intelligence (AI), and cloud computing technologies enable businesses stay competitive and increase output, productivity, and efficiency. In addition, incident response readiness, which includes the creation of incident response teams and testing incident handling plans, and security automation solutions, which include AI, analytics, and orchestration, demonstrated the highest reduction in data breach expenses (IBM Cost of a data breach report 2020). Modern technologies are used by businesses to store and process customer data as effectively as feasible. However, this results in data breaches and leaks of private information, particularly when deploying technology like AI on a broad scale.

It is important to note that businesses with a profit-driven primary goal may be more concerned with maximizing their revenues than upholding an individual's right to privacy. They may either purposefully or unintentionally collect and utilize personal data illegally. Statistics show a rise in both the quantity of fines and the total amount of fines for non-compliance with the GDPR (see figure 1, 2). However, with sufficient laws, penalties, and more public awareness, unlawful methods of gathering and processing personal data are becoming more visible to society and have a negative impact on reputations and the economy. It is fairly common for a person to passively consent to the acquisition and further monetization of their personal data while they are unaware of its value.

The protection of customer data and upholding a positive reputation are now requirements for businesses that wish to gain the trust of their clients and succeed in the market. Data breaches could seriously and perhaps permanently undermine a company's brand, especially if they are properly managed. The quantity of reported data breaches has increased after the GDPR's implementation. Risk Based Security estimates that in 2019 there were 284% more records exposed than there were in 2018 (RBS 2019). Therefore, even while preventing data breaches ought to be a top priority and no company wants a data breach, there are some situations where mistakes that result in a data breach cannot be avoided. The organization will have to invest a significant amount of money to deal with the repercussions of a data breach and try to regain the client's trust in this scenario because it will jeopardise the client's trust (Data privacy manager 2020).

An organization should prepare for a variety of outcomes that might harm its reputation in the event of a data breach, including media attention, customers and potential customers turning against it and complaining on social media, as well as eventual client loss. This in turn causes financial losses, a loss of brand value, and a loss of trust. Data breaches are expensive for a variety of reasons. The corporation will first need to deal with the costs associated with controlling the incident. Second, there are times when compensating impacted consumers is required. Thirdly, it lowers the value of the shares. Stock prices drop by about 5% when a data breach happens and personal information is made public (Ponemo 2017). The requirement to raise both short-term and long-term security expenses comes in fourth.

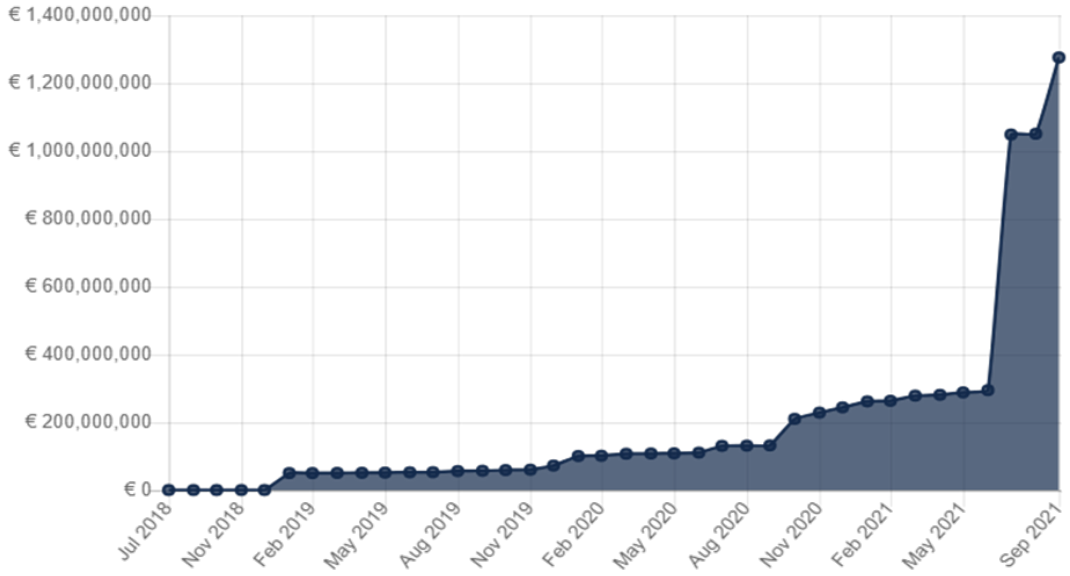

Figure 1. The overall sum of GDPR fines (cumulative). Source: (GDPR Enforcement Tracker 2021)

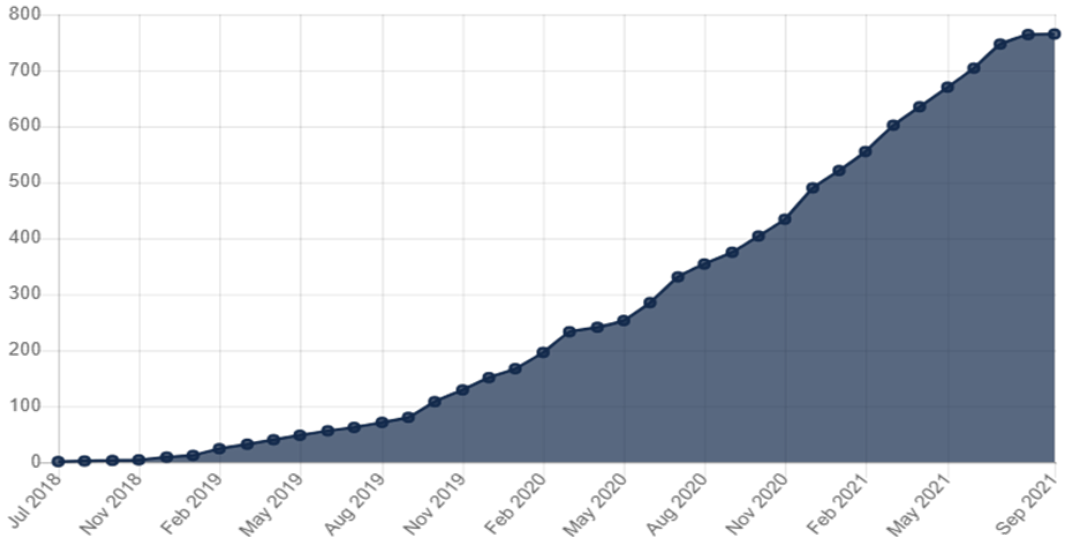

Figure 2. The overall number of GDPR fines (cumulative). Source: (GDPR Enforcement Tracker 2021)

2. Facial recognition: pros and cons

Facial recognition refers to the use of computer software to recognize or verify a person's identification using their face. It operates by recognizing and quantifying facial features in images. Facial recognition technology can recognize human faces in pictures or videos, assess whether a face appears in two different pictures of the same person, or look for a face in a big database of pictures that have already been taken (Nolan 2011). Facial recognition is a technique used by biometric security systems to more reliably identify

users during user registration or login processes. Face analysis technology is also frequently used in mobile and personal devices to ensure device security.

A wide range of applications for facial processing technology (FPT), particularly facial recognition systems, include tracking people using face identification tools, predicting the demographics of a subject group, and detecting smiles to measure customer happiness. The corporate spin on these technologies' beneficial applications includes assertions that they can "understand people", "watch or detect human activities", "index and search digital image collections", and "verify and identify subjects in security scenarios" (Clarifai 2019).

Some pros of implementing facial recognition systems into the national practice of personal identification include:

1. Enhanced security

Using facial recognition as a verification method is rapid and effective. Compared to other biometric technologies like fingerprint or retina scans, it is quicker and more practical. In comparison to typing passwords or PINs, facial recognition involves fewer touchpoints. For added security assurance, it offers multifactor authentication.

2. Greater accuracy

When identifying people, facial recognition is more reliable than using just a phone number, email address, address, or IP address. For instance, the majority of exchange services, including those for stocks and cryptocurrencies, now rely on facial recognition to safeguard clients' money.

3. Simple Integration

The majority of security software is compatible with and easily integrated with face recognition technologies. For instance, software or algorithms for facial recognition are already supported by smartphones with front-facing cameras.

The technology of facial recognition has the potential to alter our future. However, the introduction of this new system into society carries some dangers and implications, just like every innovation:

1. Concerns about privacy

Since facial recognition is not merely a passive recording, it varies from standard camera surveillance. Instead, the collected biometric information is matched to information found in databases, and the information can be effectively updated. Facial recognition data is regarded by the GDPR as "sensitive data" of personal data when it is used for identifying purposes.

2. Restricts individual freedom

Facial recognition technology might give the public the impression that they are constantly being observed and graded for their behavior when they are being recorded and scanned. Additionally, authorities can use facial recognition to put every person in their database through a fictitious criminal lineup, which is equivalent to treating you as a suspect in a crime without having any solid evidence.

3. Data breach possibility

Facial recognition data storage is also a source of worry due to the vulnerability of these databases. In the past, hackers have gained access to databases holding facial scans that have been gathered and used by banks, police forces, and defense companies. Threat actors might escalate the breach and gain access to even more sensitive data if they had facial data that was connected to a victim's phone or that was connected to information about them in a banking database.

4. Possibilities for fraud and other criminal activity

Lawbreakers can even commit crimes against innocent victims using facial recognition technologies. To perpetrate identity fraud, they can gather people's private information, including pictures and videos taken via facial scans and kept in databases. With this knowledge, a criminal may open bank accounts, obtain other loans, and use credit cards in the victim's name. Threat actors might even put someone on a criminal record in light of the usage of face recognition to add shoplifters to criminal databases that was described earlier. Beyond fraud, criminals can use facial recognition technology to harass or pursue victims. Reverse image searches could be used by stalkers on a photograph taken in a public setting to learn more about their targets and improve their treatment of them (Nolan 2011).

3. Aspects of Modern Personal Data Processing Technologies and Government Surveillance

3.1. Artificial intelligence and machine learning

Machine learning and artificial intelligence are closely related and interconnected and are also used to process big data. Despite their close connections, machine learning and artificial intelligence are not the same. A part of artificial intelligence is machine learning. The capacity of a computer system to imitate human cognitive processes like learning and problem-solving is known as artificial intelligence. A computer system can replicate human reasoning to learn from new knowledge and make judgments using AI (Duan, Edwards and Dwivedi 2019).

One use of AI is in machine learning. It is the practice of enabling a computer in learning without direct instruction by applying mathematical models of data. As a result, a computer system may keep picking up new skills and become better on its own.

Through the use of AI-based software, it is possible to design machines to behave in ways that are similar to human behavior. The activities that these AI algorithms execute are likely already preprogrammed because they were created by creators. Machine learning imitates the critical reasoning that humans employ to react to events properly.

The usage of AI-based solutions is currently widespread, ranging from project assignment based on capabilities to forecasting product demand (Gejing and Yang 2019). Industries may benefit from Machine Learning by using it to analyze vast amounts of data and combine it with human expertise to make better decisions (Ibid).

Machine learning's fundamental element is that it gains knowledge from data. This technology is widely used and can drastically reduce human workload to perform more crucial jobs. Machine learning is far more advanced than rule-based decision-making, which is used in the majority of statistical analysis. It may be used in a wide variety of business situations where the result depends on a large number of variables.

Systems that employ machine learning can learn from data, and those systems get better over time. Over time, machine learning algorithms can get more precise and effective. The algorithms improve in accuracy as the number of data increases. The neural networks utilized by ML algorithms have thousands of nodes, each of which solves a portion of the issue and transmits its results to the following node. The procedure goes on until a definitive solution is discovered.

3.2 Internet of things

Data technologies have now been widely used due to the value of the data. It is acknowledged that data created 10 years ago is significantly less useful than data created

in an hour, even though the challenge of processing hundreds of terabytes of data has been overcome. It implies that the more recent the data, the greater the value it possesses. The so-called real-time data, which are often created a few seconds from now or even less than one millisecond, are therefore the most important (Zheng et al. 2019)

Such real-time data can be obtained, for instance, utilizing the internet of things (IoT). IoT is the concept of a data transmission network between physical objects (things) equipped with built-in means and technologies for interacting with each other or with the external environment. The most popular examples are wearable objects such as smart watches or "smart house" systems. These things are able to reveal significant and sometimes very intimate information about users. They can reveal their wearers' physiological characteristics, geographical location, health condition, and health issues. Should one analyze the data provided by IoT objects, one would be able to reconstruct the environment of users. The information from the location coordinates, physiological parameters and signs of activities, current speed traveled and direction, rich high-resolution photographs, and sometimes even audio captured or voice messages allows to deduce a comprehensive picture about a user. An analysis of can be done by humans, Artificial Intelligence (AI) or AI combined with Machine Learning.

Although there are certain difficulties, enterprise IoT solutions enable businesses to enhance current business models and create new relationships with clients and partners (Ibid). A system of smart devices can create an excessive amount of data (Also known as big data). Setting up data analytics to act on huge data and integrating it into current systems can be challenging.

As a result, while developing IoT systems, security is a crucial factor since the data breach or mistakes can happen, especially if the process is poorly managed and controlled. Nevertheless, IoT has shown to be worthwhile for many businesses, and there are successful enterprise IoT use cases in almost every sector.

3.3 Big data and Big data analytics

Big Data and Big Data Analytics (BDA), along with AI, according to a number of researchers, introduces a new frontier in the way in which information can be processed and used to acquire information for decision-making (Paterson and McDonagh 2019). Big Personal Data involves the application of speedy and sophisticated data analysis to huge data sets, including data about individuals and groups of individuals, gathered from a wide range of sources. It utilizes BDA which commonly utilizes AI. As explained by the UK Information Commissioner, a significant feature of AI programs is that 'they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly'. One of the most important features inherent to AI that is used in BDA is that it creates a so-called "black box" effect since it uses complex mathematical algorithms to process data and to make decisions while the algorithms are usually non-transparent. As the name suggests, the black box effect is characterized by the absence of knowledge of its internal working processes.

As a result of digitalization and constantly appearing new data online, appeared a concept of big data. Big data is a body of information that is enormous in volume and is always expanding rapidly. No typical data management systems can effectively store or analyze this data because of its magnitude and complexity. Big data is a type of data that is extremely large.

Data flows are unpredictable, changing often and varied substantially in addition to the rising velocities and kinds of data. Businesses must understand social media trends

and how to handle peak daily, seasonal, and event-triggered data loads, which can be difficult (Gupta and Rani 2019).

Another important parameter is data quality which is referred to as veracity. It is challenging to link, match, clean up, and convert data across systems since it originates from so many distinct sources (Ibid). Relationships, hierarchies, and numerous data links need to be connected and correlated in business. If not, their data might easily spin out of control.

Big data allow businesses to use external intelligence when making choices thanks to big data analysis, which has a number of advantages. Organizations can refine their business strategy thanks to the availability of social data from search engines and websites like Facebook and Twitter (Ibid).

Big data analytics involves applying cutting-edge analytical methods to very large, diversified big data sets, which can range in size from terabytes to zettabytes and contain organized, semi-structured, and unstructured data from many sources.

The big data analytics technology is a synthesis of several approaches and processing strategies. Their combined usage by businesses to get pertinent outcomes for strategy management and implementation is what makes them effective.

Organizations may access a huge amount of data and analyze data from many different sources to learn new things and take action. Organizations may save money by using adaptable data processing and storage systems to store and analyze massive amounts of data (ibid). Find trends and insights that will help you run your business more effectively. A company may become data-driven by analyzing data from sensors, devices, video, logs, transactional apps, the web, and social media (Shakhovska, et al.2019). It also enables to assess the implications and demands of the market when you develop new goods and services.

Better customer service: Big Data technologies are being used to create new systems that will eventually replace outdated consumer feedback methods. Big Data and technology for natural language processing are being employed in these new systems to read and assess customer feedback.

3.4 Artificial intelligence and machine learning

Machine learning and artificial intelligence are closely related and interconnected and are also used to process big data. Despite their close connections, machine learning and artificial intelligence are not the same. A part of artificial intelligence is machine learning.

The capacity of a computer system to imitate human cognitive processes like learning and problem-solving is known as artificial intelligence. A computer system can replicate human reasoning to learn from new knowledge and make judgments using AI (Duan, Edwards and Dwivedi 2019).

One use of AI is in machine learning. It is the practice of enabling a computer in learning without direct instruction by applying mathematical models of data. As a result, a computer system may keep picking up new skills and become better on its own.

Through the use of AI-based software, it is possible to design machines to behave in ways that are similar to human behavior. The activities that these AI algorithms execute are likely already preprogrammed because they were created by creators. Machine learning imitates the critical reasoning that humans employ to react to events properly.

The usage of AI-based solutions is currently widespread, ranging from project assignment based on capabilities to forecasting product demand (Gejing and Yang 2019).

Industries may benefit from Machine Learning by using it to analyze vast amounts of data and combine it with human expertise to make better decisions (Ibid).

Machine learning's fundamental element is that it gains knowledge from data. This technology is widely used and can drastically reduce human workload to perform more crucial jobs. Machine learning is far more advanced than rule-based decision-making, which is used in the majority of statistical analysis. It may be used in a wide variety of business situations where the result depends on a large number of variables.

Systems that employ machine learning can learn from data, and those systems get better over time. Over time, machine learning algorithms can get more precise and effective. The algorithms improve in accuracy as the number of data increases. The neural networks utilized by ML algorithms have thousands of nodes, each of which solves a portion of the issue and transmits its results to the following node. The procedure goes on until a definitive solution is discovered.

4. Conclusions

Facial recognition technology may boost security and, in some situations, can be used to respond to a public health emergency and make some places even safer. However, the ethical and sociological hazards that could violate norms and principles commonly accepted in liberal democracies were highlighted by the problematic aspects of facial recognition applied in public places. It is still not practical to employ facial recognition on a broad scale in Europe due to a number of ethical and legal issues (particularly compliance with privacy laws). The drawbacks and dangers of facial recognition technology may be lessened as it advances, but legal problems are certain to persist.

The most advantageous information is found in real-time data, which may be used to depict fraudsters' shifting patterns or to reflect customer preference changes. Promoting real-time stream data technology is increasingly important. Whether it is connected to health, marketing, entertainment, or any other industry involving the exploitation of data or information in some manner, data processing technologies have resulted in a shift in practically every one of these areas. Every small and large-scale firm or organization is now concerned with comprehending the idea of big data and using it effectively to boost productivity.

The constantly expanding data presents both possibilities and difficulties for data collection, storage, manipulation, administration, analysis, knowledge extraction, security, privacy, and visualization. Due to Big Data, sophisticated algorithms, more processing power, and better storage, AI has grown in popularity today. As a result, AI systems are now becoming an integral part of digital systems and, more particularly, have a significant influence on human decision-making. As a result, there is a growing need for information systems researchers to look into and comprehend how data processing technologies affect decision-making, as well as to contribute to the development of data processing technologies theoretical aspects as well as the success of implementation of these technologies in practice.

References

Altieri, L. and Cifaldi, G. (2018) ”Big data, privacy and information security in the European Union”, *Sociology and Social Work Review,* vol. 2, no. 1, 56-64.

Duan, Y., Edwards, J. S., and Dwivedi, Y. K. (2019) ”Artificial Intelligence for decision making in the era of big data – evolution, challenges and research agenda”,

International Journal of Information Management, 48, 63-71. doi:10.1016/j.ijinfomgt.2019.01.021

Gejing, X. and Yang, L. (2019) Research on the impact of internet evolution on accounting information system based on Data Mining. Journal of Physics: Conference Series, 1345(5), 052055. doi:10.1088/1742-6596/1345/5/052055

Gupta, D. and Rani, R. (2018) "A study of Big Data Evolution and research challenges", *Journal of Information Science*, 45(3), 322–340. https://doi.org/10.1177/0165551518789880

Nolan, J. (Executive Producer). (2011-2016) *The person of interest* [TV series]. Kilter Films.

Paterson, M. and McDonagh, M. (2019) "Data Protection in an Era Of Big Data: the Challenges Posed By Big Personal Data", *Monash University Law Review*, Vol 44, No 1.

Shakhovska, N., Boyko, N., Zasoba, Y. and Benova, E. (2019) "Big Data Processing Technologies in distributed information systems", *Procedia Computer Science*, 160, 561–566. https://doi.org/10.1016/j.procs.2019.11.047

Zheng, T., Chen, G., Wang, X., Chen, C., Wang, X. and Luo, S. (2019) "Real-time Intelligent Big Data Processing: Technology, platform, and applications", *Science China Information Sciences*, 62(8). https://doi.org/10.1007/s11432-018-9834-8

Clarifai (2019) Custom Face Recognition. https://www.clarifai.com/custom-face-recognition [accessed 31 Oct. 2022].

CMS (2021) GDPR Enforcement Tracker Report 2021. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report [accessed 1 March 2022].

IBM (2020) How much does a data breach cost? from https://www.ibm.com/security/data-breach [accessed 13 July 2022].

Ponemon. (2017) The Impact of data breaches on reputation & share value. https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf [accessed 24 July 2022].

Risk based security (2019) Q3 2019 Data Breach QuickView Report. https://www.internetworldstats.com/stats.htm [accessed 11 July 2022].

The Chartered Institute of Marketing (2016) Be transparent on social media or risk the consequences. https://www.cim.co.uk/newsroom/opinion-be-transparent-on-social-media-or-risk-the-consequences/ [accessed 12 July 2022].

The Economist (2017) The world's most valuable resource is no longer oil, but data. May 6th, 2017 edition. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [accessed 21 June 2022].

Received 21 august 2022, accepted 11 December 2022