December 6, 2024

Behind the Scanner: The Amazon Case and the Conflict Between Productivity and Privacy

Final Exam Paper

Datafication: Regulation, Governance, Security, Privacy and Ethics

Program: MSc in Business Administration and Data Science

Authors: Ludovico Francia (177119), Michele Daconto (176193)

Examiner: Max Gersvang Sørensen

Number of characters: 19.715

Number of pages: 10

Academic Year 2024/2025

Table of Contents

1. Introduction 1
2. Indicators in breach 2
  2.1 Stow Machine Gun 3
  2.2 Idle Time and Latency Time 4
3. The Unlawfulness of the 31-Days Retention 5
4. Obligation to Inform Temporary Workers 6
5. Infringements Relating to Video Surveillance Processing 7
  5.1 Failure to Inform Data Subjects 7
  5.2 Failure to Implement Sufficient Data Security Measures 7
6. Corrective Measures and Fine 8
7. Conclusion and Ethical Considerations 9
References 11

1. Introduction

Amazon France Logistique (AFL) is the engine of the U.S. giant Amazon.com Inc's logistics operations on the French territory. This division is responsible for the distribution of tens of thousands of items purchased daily on the Amazon.fr portal. AFL is fully controlled by Amazon.com Inc through the European headquarters of Amazon EU Sarl, based in Luxembourg. With more than 6.200 permanent employees and more than 21.000 temporary workers (2019 figures), AFL handles the entire lifecycle associated with a product order: storage, preparation, and shipping.

The operations conducted by AFL are characterized by the use of advanced technological systems designed to increase the efficiency, safety and quality of warehouse management through the analysis of a large amount of data, both personal and non-personal. However, the processing of personal data, relating to customers and employees, should result in Amazon taking a particularly high degree of care in their use.

After several journalistic inquiries and reports from employees, the French Data Protection Authority (CNIL), in Decision No. 2019-187C dated September 26, 2019, decided to assess AFL's compliance with the General Data Protection Regulation (GDPR), focusing on the processing of employees' personal data. CNIL President Alexandre Linden first ordered inspections at AFL's various

administrative offices and warehouses and then initiated a written investigation, conducted through a continuous exchange of information with AFL, during the period between November 2019 and January 2021. On January 28, 2021, the CNIL president appointed Mr. François Pellegrini as rapporteur with the task of reviewing the evidence collected and proceeding with an evaluation of the case. The massive processing of data is crucial to ensure the efficiency and competitiveness of logistics giant Amazon but raises questions about the balance between innovation and regulatory compliance.

The investigation concluded on December 27, 2023, with the publication of the Délibération SAN-2023-021 issued by the Commission National de l'Informatique et des Libertés. In this resolution, the CNIL imposed a penalty of €32 million on AFL for multiple violations of key GDPR principles, including lack of an adequate legal basis, failure to ensure data minimization, insufficient transparency, and inadequate security measures.

In addition to the regulatory aspect, the AFL case raises important ethical issues. The violations found during the investigation not only compromise the privacy of workers but also raise concerns about the protection of their dignity and fundamental rights. At a time when the processing of personal data plays an increasingly central role, this case invites us to reflect on the responsibility of businesses to balance their economic interests with the protection of people’s rights.

This synopsis aims to analyze the problems identified in Amazon France Logistique's processing of personal data in light of GDPR principles, offering a reflection on how these breaches have challenged the company's right to process employee data to maximize the efficiency of its logistics system.

2. Indicators in breach

The main objective of the report submitted to the AFL on 4 April 2022 by Mr. Pellegrini, the rapporteur of the CNIL’s investigation, is to investigate the lawfulness of the indicators collected by the company to monitor the quality and productivity of each employee's work. These metrics are accessible in real-time through computerized tools by line managers, who also have access to a daily performance report for each of their employees, in addition to being able to consult the data for up to 31 days after its collection.

Among the over 50 indicators used by the company, the legitimacy of which has been challenged by the CNIL's auditors, the rapporteur believes that three of them do not comply with Article 6 of the GDPR.

AFL responded to these allegations with two statements, the first in June 2022 and the second in May 2023. In these communications, the company stated that the indicators in question — the Stow Machine Gun, Idle Time, and Latency Time of Less Than Ten Minutes — were collected to ensure greater employee safety and to optimize their workload through departmental redistribution. Despite the AFL's clarification that these tools were not intended to pressure employees into working more intensively, it is known that some employees received awareness-raising letters urging them to increase their productivity.

Let’s analyze these indicators. For simplicity, we have combined the Idle Time and Latency Time into a single paragraph, as the objections raised by the supervisory authority against them were very similar.

2.1 Stow Machine Gun

The Stow Machine Gun measures the time elapsed between one scan and the next performed by an employee. It is a quality indicator designed to monitor human errors that could potentially compromise product quality. The process of evacuating an item requires the operator to perform specific actions, and if the time between scans is too short (< 1.25 seconds), it is highly likely that an error has been made.

2.1.1 Non-Compliance with GDPR

The French supervisory authority deemed the Stow Machine Gun to be highly intrusive, as it can monitor every employee’s action almost to the second. This level of monitoring exceeds the reasonable expectations of workers, who are aware that they are being monitored but do not expect such a high level of precision. It is likely that the processing of this indicator could have negative moral repercussions on employees and violates their right to privacy at work (Article L1121-1, French Labour Code, n.d.).

Within the scope of Article 6(1)(f) of the GDPR, the restricted committee, in coordination with the rapporteur, believe that the rights and freedoms of the data subjects (employees) outweigh the legitimate interest of the controller in ensuring greater safety and efficiency. Furthermore, the principle of data minimization was compromised as such granular data were not strictly necessary.

For these reasons, the processing of the Stow Machine Gun lacks a legal basis, constituting a breach of Article 6(1)(f) of the GDPR.

2.1.2 AFL's proposed resolution

In one of the statements issued by Amazon Europe in response to the allegations, the company indirectly attempted to negotiate by promising to stop processing this indicator. However, in its final deliberation the CNIL made it clear that this does not relieve the company of its responsibility for past infringements.

2.2 Idle Time and Latency Time

The Idle Time indicator records any unjustified inactivity of a worker exceeding ten minutes. This can manifest in three possible scenarios: (1) the employee encounters a technical problem, (2) the employee requires assistance, or (3) the employee takes excessive unauthorized breaks outside of designated break times.

Latency Time for Less Than Ten Minutes is an even more specific index than Idle Time, as it measures instances of unjustified scanner inactivity lasting less than ten minutes during critical moments of the day, such as the start or end of a shift or the resumption of work after a break.

2.2.1 Non-Compliance with GDPR

According to the CNIL, the processing of these two indicators in this way is excessively invasive, as it potentially requires employees to justify every moment that is deemed non-productive. The commission also noted that these indicators make it possible for line managers to track the number of minutes that elapses between the time an employee enters the site and the time of the first scan.

Once again, Article 6 of the GDPR applies as the employee's right to privacy outweighs the controller's legitimate interest. Therefore, the two indices do not comply with the principles of the GDPR.

2.2.2 AFL's proposed resolution

In the same statement in which AFL announced that it would no longer use the Stow Machine Gun indicator, the company also promised to raise the threshold for idle and latency time from 10 to 30 minutes. In addition, these indicators would only be displayed on computerized tools and made accessible to line managers after a two-hour delay.

These new less intrusive measures were welcomed by the restricted commission, although it stressed that these adjustments do not absolve the company of its responsibility for past violations.

3. The Unlawfulness of the 31-Days Retention

The French authority considered the 31-day retention period for individual employee data on productivity and quality indicators to be disproportionate. While AFL argued that the retention of detailed data for such a period was essential for operational efficiency, the CNIL concluded that a shorter retention period, such as one week, would be more than sufficient to achieve this purpose. In addition, the Commission considered that access to extensive historical data - down to hourly detail - was excessive and intrusive, especially when simpler and less intrusive solutions could achieve the same objectives.

In the May 2023 statement, AFL agreed to accept the proposal to reduce the 31-day retention period to 7 days and to aggregate data on a weekly basis. Anyway, this compromise does not absolve the company of its past responsibilities.

This practice violated the principle of data minimization under Article 5(1)(c) of the GDPR, which requires personal data to be adequate, relevant and limited to what is necessary for the purposes of processing. The retention of such a large amount of detailed personal data increased the risks to employees' privacy and may have a negative impact on their morale, undermining their right to fair working conditions.

4. Obligation to Inform Temporary Workers

AFL made the policy regarding the processing of data collected through scanners available to temporary workers, about 20.000 in 2019, via the company intranet. The CNIL judged this as not sufficient to be compliant with Articles 12 and 13 of the GDPR.

These articles require that “the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form [...]” and that “[...] the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information [...]”.

AFL challenged this violation by pointing out that the GDPR itself in Article 12 allows to inform “[...] in writing, or by other means, including, where appropriate, by electronic means.”

However, the restricted panel pointed out that it is not questioning the means used, which turns out to be legitimate, but the way they interfaced with the data subject. The workers were neither directly provided with a privacy policy nor given an invitation to view the privacy policy available on the company intranet.

The lack of proactivity on the part of the company, according to the select committee, did not constitute a “satisfactory means of information” under GDPR standards.

Following these findings, AFL began remediation in April 2020: it required temporary employment agencies to provide employees an additional privacy statement regarding the processing of performance indicators.

By failing to put these measures in place “at the time when personal data are obtained,” as required by Article 13 of the GDPR, the select committee determined that through April 2020 AFL's practices violated Articles 12 and 13 of the GDPR.

This failure on the part of AFL underscores the centrality of the data subject's role in the processing of personal data. The data subject must be proactively informed by the data subject prior to the collection of their data. Merely making information passively available is not sufficient to meet the transparency and accessibility requirements expressed by the GDPR.

5. Infringements Relating to Video Surveillance Processing

5.1 Failure to Inform Data Subjects

Article 13 of the GDPR states that "[...] the controller shall, at the time when personal data are obtained, provide the data subject with all the following information: [...]". Among the information to be given to the data subject are the contact of the data protection officer, the data retention period and the right to lodge a complaint with a supervisory authority.

Following the inspections of Lauwin-Planque and Montélimar carried out in November 2019, the rapporteur noted that the measures implemented by the establishments were not compliant with the standards required by Article 13 of the GDPR. These establishments used a video surveillance system but, in addition to reporting its presence, workers were not given any of the information indicated by Article 13 of the GDPR.

In its defense, the company claimed to be compliant with the CNIL recommendations dated 2015. The panel rejected this objection, pointing out that the GDPR had been in force for more than a year and a half at the time of the inspection and therefore it was the company's responsibility to comply with Article 13.

The panel therefore found AFL liable for violating Article 13 of the GDPR by failing to provide the necessary information to data subjects.

5.2 Failure to Implement Sufficient Data Security Measures

The warehouses inspection found two critical practices that compromise the level of security associated with the data processed by the video surveillance system. Most of the video surveillance images at the Montélimar site were accessible to authorized persons through a single shared account. In addition, a 12-character password with only lower-case letters and numbers was required to access this account, a password that in the eyes of the restricted panel was not sufficiently robust.

The restricted panel recalls that it follows from article 32 of GDPR that “the controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.”

In this case, the company does not dispute the breach but argues that the breach can be attributed to the software supplier of the video surveillance system. According to the company, the supplier would have designed the software in such a way that sharing of only one account was unavoidable. As for the non-robustness of the password, the company claims that it is compensated by the presence of a previous password required to access the Windows account.

As for sharing a single account, the select committee recalls that the 2018 recommendations published by the CNIL explicitly call for a "unique identifier per user" and prohibit shared access among multiple users. The use of a unique identifier is essential to allow the attribution of each action performed on a computer to a specific person. A shared account can, for example, compromise investigations in case of fraudulent access or elimination of images. The company had an obligation to contact the software supplier and request a software modification to allow multiple accounts.

With regard to the insufficient robustness of the password, the restricted panel points out how this can be easily circumvented with "brute force" or "dictionary" attacks. The 2022 CNIL resolution recommended that the password should have at least three of the following types of characters: lower case, upper case, numbers and special characters. The use of prior authentication using Windows accounts is not deemed sufficient by the restricted panel because the software was accessible from as many as 7 different computers and 22 people.

Consequently, the restricted panel found that the use of a shared account among multiple users and an insufficiently strong password violated Article 32 of the GDPR.

6. Corrective Measures and Fine

On the basis of the report prepared by Mr. Pellegrini and after hearing several AFL spokesmen, the restricted committee decided, on 27 December, to impose a sanction.

From an analysis integrating Article 83 of the GDPR with Law No. 78-17 of January 6, 1978, of the French Data Protection Act, we can understand how this sanction was formulated. Article 83(4)(5) of the GDPR stipulates that for less severe cases, the maximum fine applicable to a company corresponds to the higher of €10 million or 2% of the worldwide annual turnover of the previous

financial year. For more severe cases, involving violations of Articles 5 or 6 of the regulation, these maximum limits are increased to €20 million and 4%, respectively.

In any case, the sanction must always be effective, proportionate and dissuasive.

As AFL's breaches of Articles 5(1)(c) and 6 of the GDPR are both frequent and particularly serious, this case falls under the second category.

At the end of his report, Mr. Pellegrini had proposed to the restricted committee that the maximum fine could be calculated based on the turnover of the entire economic unit, Amazon.com Inc. This proposal was considered "illegal" by the company's spokespersons, as the investigations had consistently referred only to Amazon France Logistique and not to Amazon.com Inc. as a whole. The committee agreed with the AFL's legal representatives.

With a turnover of €1.135 billion in 2021, AFL faced a maximum possible fine of €45.4 million (4%). The commission determined that a fine of €32.000.000 (thirty-two million euros), equivalent to nearly 3% of the company’s 2021 turnover, would be appropriate in AFL's case. This significant sanction considers also the competitive advantage AFL allegedly gained over other online shopping companies through invasive practices affecting its workers.

The decision will remain public for two years and will include AFL's name. After this period, it will still be available but will no longer be attributed to the company. AFL objected, arguing that the decision contained too much detail about the tools that the company uses and that even after two years there would still be numerous journalistic articles on the matter. The Commission answered that publication was fully justified by the seriousness of the breaches in question and the significant number of people affected.

7. Conclusion and Ethical Considerations

The decision of the Commission Nationale de l'informatique et des libertés on Amazon France Logistique brings to the forefront the ethical debate on how to balance efficiency and protection of workers' fundamental rights.

The CNIL challenges neither AFL's right to ensure productivity, quality, and safety in its operations nor the strategic value of monitoring systems for managing warehouses. However, in evaluating each issue the CNIL brings to the forefront the principle of balancing, recognized in Article 6(1)(f) of the GDPR, between these interests and employees' rights to privacy and dignity.

Regarding the use of indicators to monitor aspects such as productivity and quality of operations, the constructive approach taken by the CNIL is noticeable. It does not simply denounce the disproportionate practices adopted by AFL but proposes concrete alternatives for GDPR compliant data processing. Among the recommendations we find the use of aggregate indicators, which reduce the identifiability of individual workers and compliantly allow the pursuit of legitimate interests such as the productivity, quality and safety of AFL operations.

From an ethical perspective, this decision invites us to ponder the following question: how far can the pursuit of efficiency by means of new technologies go without infringing on workers' fundamental rights? In this merit, the CNIL decision is a call to all companies to promote management models that are sustainable, where technology is used not as a tool of oppression but as a tool of support.

References

- About Amazon EU, *Statement on the CNIL Deliberation*, January 22, 2024. https://www.aboutamazon.eu/news/policy/amazons-statement-on-the-cnil-deliberation

- CNIL, *Délibération SAN-2023-021 du 27 décembre 2023 concernant la société Amazon France Logistique*, January 23, 2024. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000048989272

- European Data Protection Board, *Employee monitoring: French SA fined Amazon France Logistique €32 million,* January 23, 2024. https://www.edpb.europa.eu/news/national-news/2024/employee-monitoring-french-sa-fined-amazon-france-logistique-eu32-million_en

- European Parliament and Council, Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), May 4, 2016. https://gdpr-info.eu

- Marassi, S. & Bolte, J., *Leveraging Data Protection Law for Protecting Workers' Fundamental Right to Health and Safety in the Workplace: The Amazon Case*, *International Labor Rights Case Law*, June 24, 2024. https://brill.com/view/journals/ilrc/10/2/article-p263_021.xml

- République Française, *Code du travail*, Article L1121-1, March 12, 2007. https://french-business-law.com/french-legislation-art/article-l1121-1-of-the-french-labour-code/

- Trzaskowski, J. & Sørensen, M. G. (2019). *GDPR Compliance: Understanding the General Data Protection Regulation*, Ex Tuto Publishing.

- Data Privacy Manager, *€32 million GDPR fine for Amazon France Logistique*, January 24, 2024. https://dataprivacymanager.net/e32-million-gdpr-fine-for-amazon-france-logistique/