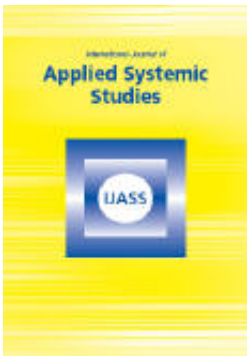

International Journal of Applied Systemic Studies

ISSN online: 1751-0597 - ISSN print: 1751-0589
https://www.inderscience.com/ijass

Postal sector digitalisation: security and vulnerabilities

Aikaterina Papanikolaou, Eleni Varvarousi, Eirini Gavala

DOI: 10.1504/IJASS.2024.10064596

Article History:

Received:	14 December 2022
Last revised:	15 December 2022
Accepted:	26 September 2023
Published online:	25 June 2024

Postal sector digitalisation: security and vulnerabilities

Aikaterina Papanikolaou, Eleni Varvarousi* and Eirini Gavala

Hellenic Authority for Communication Security and Privacy (ADAE), Ierou Lochou 3, Maroussi 151-24, Athens, Greece
Email: aikaterina.papanikolaou@gmail.com
Email: varvarousie@adae.gr
Email: igavala@adae.gr
*Corresponding author

Abstract: The postal sector has seen a significant transformation throughout the years facing various challenges and opportunities. The development of e-commerce has led to an increase in parcel delivery services, hence generating innovative delivery alternatives and business models that have had a profound impact on the postal sector. The significant modifications along with the process of digitisation, highlight the need of fortifying a security-oriented culture. The fundamental values of security and confidentiality of postal communications are considered inviolable, requiring postal operators to rigorously enforce security measures while handling postal items. The role of education and training of postal and courier employees is also essential and can lead to the development of confidentiality and privacy aware staff culture inseparably connected to high quality postal and courier services. Associated protective measures, response planning and training of staff can lead towards secure organisations. Furthermore, compliance with technical standards can benefit customers and lead towards a more secure postal sector.

Keywords: confidentiality; digitisation; security.

Reference to this paper should be made as follows: Papanikolaou, A., Varvarousi, E. and Gavala, E. (2024) 'Postal sector digitalisation: security and vulnerabilities', *Int. J. Applied Systemic Studies*, Vol. 11, No. 1, pp.42–51.

Biographical notes: Aikaterina Papanikolaou is a former member of the Plenary Board of the Hellenic Authority for Communication Security and Privacy (ADAE) and an expert at the Greek Ombudsman.

Eleni Varvarousi is the Head of the Department for Regulatory Framework, Monitoring New Technologies and Applications in the Division for the Assurance of Privacy of Postal Communications at the Hellenic Authority for Communication Security and Privacy.

Eirini Gavala is the Head of the Division for the Assurance of Privacy of Postal Communications at the Hellenic Authority for Communication Security and Privacy (ADAE).

1 Introduction

The fundamental right to confidentiality in communications is a cornerstone of both European Union (EU) law and international law. There is an establishment of a robust legal framework in the EU and at international level for protecting the confidentiality of electronic and postal communications. This legal framework is continuously evolving to address new challenges and technological developments, ensuring that the right to communication confidentiality remains protected in an ever-changing digital landscape.

The EU postal and delivery sector has changed dramatically throughout the years, facing many challenges and prospects. Digital transformation, the replacement of letter mail by electronic communication, the increasing importance of e-commerce which led to an increase in parcel delivery services, along with other aspects linked to postal infrastructure have had a significant impact on the postal sector. Technology trends such as blockchain, interactive AI, quantum computing, cloud computing, big data analytics, digital twins, indoor mobile robots, are key enablers for the postal sector. Posts' strategic objectives are undergoing significant transformation because of these technological developments, which necessitate enhanced predictability, transparency, security and efficiency in order to satisfy new customer demands. Furthermore, the demand for parcel and e-commerce related mail services which increased at an accelerating rate among the EU-27 member countries during the pandemic created changes in user needs (European Commission, 2022b). Furthermore, it is noteworthy that the online retail sector has shown stability in many EU member states throughout the year 2022. This is particularly notable given the initial anticipation that the e-commerce industry would see a substantial deceleration after the lifting of COVID-19 pandemic limitations (Lone and Weltevreden, 2022). The above developments affected not only the postal and courier operators but also the competent and supervisory authorities in EU-27, responsible for monitoring and auditing the postal and courier sector. These changes have shown not only the complexities of the postal network but also created the need to establish further a culture of postal security by enhancing the collaboration among the member states. Moreover, they have demonstrated the importance of education of the postal and delivery sector workforce to facilitate postal development and maximise safety and quality of postal services.

2 The legal principle of security of correspondence

The secrecy of correspondence is a fundamental legal principle. Almost all European constitutions contain a right protecting the confidentiality of communications. The principle naturally extended to other forms of communication, including electronic communications, as the constitutional guarantees cover these forms of communication as well. Secrecy of correspondence signifies the inviolability of postal communications relating to letter post, and parcels. This fundamental principle guarantees that the content of sealed letters/packets/parcels is never revealed and opened by any officials or any party. The right of privacy to your own letters is the main legal basis for the assumption of privacy and secrecy of correspondence. In the European Convention on Human Rights, Article 8, encompasses the right to respect private and family life, home, correspondence. Furthermore, in the Universal Postal Convention, it is stated that member countries and

their designated operators shall ensure the confidentiality and security of personal data on users, in accordance with their national legislation (Universal Postal Union, 2019).

The secrecy of correspondence is enshrined in the constitutions of several European countries. The Constitution of Greece, as revised by the parliamentary resolution of 27th May 2008, of the VIII the Revisionary Parliament, protects in Article 19 the classic right to secrecy of correspondence. Confidentiality in the postal sector is characterised as the obligation of postal enterprises and their staff to refrain from providing any unauthorised person with any information that comes to their attention from handling mail items or to refrain from enabling an unauthorised person to have access to this information. Furthermore, security is characterised as the degree of protection against danger, damage, loss, and crime and refers to safeguarding the postal service. Security consists of ensuring the prevention of any breach, loss, illegal ownership, alteration of the contents of the postal item, as well as the avoidance of the transport of dangerous objects or prohibited substances (Hellenic Authority for Communication Security and Privacy, 2005). The necessity to broaden and modify the EU postal framework is significant, given the dynamic nature of the postal and supply chain sector, particularly in light of technological progress and shifting consumer preferences. Revision of the EU postal framework in these domains would necessitate a collaboration of postal operators, EU institutions, and other interested parties in a coordinated effort. It is essential to ensure that the postal system remains robust, efficient, and capable of meeting future opportunities and challenges, despite the challenges of the endeavour.

3 The Hellenic Authority for Communication Security and Privacy

The establishment of the Hellenic Authority for Communication Security and Privacy (ADAE) is in accordance with the provisions outlined in Article 19, Paragraph 2 of the Hellenic Constitution. According to Article 1 of Law 3115/2003, the primary objective of this legislation is to safeguard and preserve the correspondence or communication in any possible way. The Hellenic Authority for Communication Security and Privacy's Division for the Assurance of Privacy of Postal Communications is tasked with the following responsibilities, among others: assessing the impact of information and communication technologies (ICTs) on postal and courier services, overseeing postal service and delivery providers, evaluating the effects of standards and specifications pertaining to postal and courier companies; ensuring the confidentiality of mail services; and introducing and implementing measures to protect privacy.

Additionally, the authority carries out audits according to the applicable legislation. The audit team performs inspections at the sites of Postal Enterprises to assess the degree to which the procedures outlined in the security policy are implemented. Moreover, the authority attends to matters pertaining to proceedings of administrative bodies, legal counsel, or any other individual it deems qualified to assist in the pursuit of the ADAE's objectives. ADAE recommends the confiscation of methods of breaching confidentiality as it deems appropriate, or the obliteration of data or evidence acquired through a breach of communication privacy. ADAE issues legislative acts pertaining to privacy security in general, which are published in the Greek Government Gazette. Penalties are imposed for breaching privacy laws. ADAE's Regulation for the Assurance of Privacy in Postal Services establishes the obligations of postal enterprises, of the staff they employ, as well as of third parties who collaborate with them under any legal relationship for the

provision of postal services, with respect to confidentiality and security of postal services. ADAE also establishes a procedure for controlling whether the natural or legal persons referred to above have complied with their obligations. Violating confidentiality is a punishable offence punishable by both criminal and administrative sanctions in Greece. Criminal penalties include at least one year of imprisonment and a fine ranging from €15,000.00 to €60,000.00. Furthermore, in cases of administrative penalties, the fine can range from €15,000.00 to €1,500,000.00.

During the period ranging from 2019 to 2023, the authority imposed sanctions onto postal and courier operators for a variety of violations. These include instances of insufficient security measures and incorrect handling of postal items, as well as incidents of lost or breached mail items, unsuitable packing, and a lack of mechanisms for privacy assurance (ADAE, 2021). Moreover, the authority has levied sanctions against organisations that obstruct its auditing, process evaluation and analysis activities. The authority considers various factors, including the principles of effective administration, legality, fairness, proportionality of the companies.

4 Security audits and vulnerabilities in the postal sector

The postal network is characterised by vulnerabilities. Those vulnerabilities may be seen at all stages of the network. Specifically, vulnerabilities are seen during induction, transport as well as delivery. Most of the postal infrastructure is characterised as vulnerable. The entry point of the postal supply chain (mailboxes and post offices) and the sorting centres of mail and parcel items are considered as vulnerable. According to the Regulation of the Hellenic Authority for Communication Security and Privacy, the vulnerabilities are mainly identified at the following cases:

1 at the points of depositing the items, at the local offices of the Postal Enterprises and in the outdoor mailboxes or letter plates

2 at the points of deposition of postal items in the premises of the Postal Enterprises for further management (sorting, transport, distribution)

3 at the transfer to and from the management (sorting) centres

4 at the points of delivery of postal items.

The Hellenic Authority for Communication Security and Privacy (ADAE) receives complaints on mishandling or loss of postal items and conducts security audits accordingly. Based on the audits that the Hellenic Authority for Communication Security and Privacy has conducted, there are many complaints related to breaches of confidentiality at the sorting procedure or at the deposition of mail items. In addition, ADAE has received further complaints pertaining to postal workers, couriers, or post office clerks that fail to deliver mail goods under secure circumstances or engage in careless delivery practices. Specifically, the authority has investigated complaints regarding the inappropriate packing of postal items that reach at their destination damaged, in addition to complaints that involve delivery that takes place utilising non-secure transportation trays. Considering the information presented above, it is imperative that the appropriate precautions be taken to prevent breaches of confidentiality, unlawful ownership and alterations of the contents of postal items. For

example, to avoid the possibility of an item being lost, delivery services should ensure that mailed items are placed in the recipients' mailboxes or that items are delivered in closed, secure trays. Furthermore, postal enterprises need to take appropriate actions for safeguarding the confidentiality as well as secrecy of postal items as well as for avoiding delivery of dangerous goods. Obligations of postal enterprises or of the staff they employ and of third parties who collaborate with them under any legal relationship as the provision of postal services should be bound with confidentiality and security of postal services.

Postal enterprises must also comply with the principle of proportionality when taking measures to prevent the transport of objects dangerous to public health and safety, or of prohibited substances, so that controls carried out are not disproportionately burdensome to confidentiality regarding the intended result. Preventative measures taken by postal enterprises include locked and secured postal vehicles to prevent acts of breach of confidentiality. Furthermore, other measures concern the handling of mail items which are not delivered to the recipient's hands. If there are no mailboxes available, it is necessary to securely deposit postal items in a location that is both visible to the intended receiver and ensures confidentiality and prevention of item loss, demonstrating sufficient diligence and care. Furthermore, when exploring alternative delivery options, like parcel lockers, it is important to consider appropriate measures that align with the security and convenience needs of both the sender and the recipient. This approach helps maintain the integrity of the postal system and ensures a reliable and efficient delivery process. For users of postal services, it is imperative to adopt essential self-protection measures. These measures are crucial for safeguarding the confidentiality of correspondence. In doing so, they must exercise professional discretion to prevent unauthorised access or exposure of sensitive information. This involves being vigilant about where and how they send and receive mail, ensuring it is done in a secure manner. It is also important for users to stay informed about the best practices in mail handling and to be aware of potential risks. By taking these proactive steps, users can significantly contribute to the overall security and integrity of the postal system, ensuring their personal and professional correspondence remains private and protected.

Additionally, it is crucial for users of postal services to supply accurate recipient information. This practice is key to preventing mis-delivery and the potential risk of breaching confidentiality. Furthermore, it is imperative for users of postal services to package their mail items meticulously, adhering to the guidelines provided by postal service providers. Proper packaging is essential not only to prevent damage to the contents during transit but also to ensure discretion. Careful handling is a key aspect of maintaining the confidentiality and integrity of the contents.

In addition, it is equally important for postal providers to maintain discretion regarding the information related to their mail items. This means avoiding the disclosure of any details about the contents, destination, or origin of the mail to unauthorised or third parties. Keeping such information confidential helps prevent potential security breaches and protect sensitive information. Lastly, the importance of developing soft and digital skills among postal sector personnel cannot be overstated. In an increasingly digital world, these skills are crucial for the workforce to stay relevant and adaptable. Soft skills enhance customer service and operational efficiency. Meanwhile, digital skills are vital for managing new technologies and systems that are becoming integral to modern postal services. By fostering these skills, postal workers can better respond to

changing customer needs and technological advancements, ensuring the postal service remains efficient, reliable, and secure in a rapidly evolving digital landscape.

5 Digital transformation in the postal sector

Digital transformation is affecting greatly the postal sector which has experienced massive changes over the past decade. The European Commission proposed to establish a digital compass to interpret a vision for Europe's digital transformation by 2030 (ADAE, 2021). This vision that forms part of Europe's Digital Compass for the EU's digital decade evolves around four cardinal points: skills, government, infrastructures, and business. Furthermore, the framework of digital principles that will help to promote EU values in the digital space contains digital rights based on the protection of personal data and privacy in a secure and trusted online environment. Even though policy reform based on digitalisation began in the past decade with policy reform initiatives such as the Data Governance Act, the Digital Services Act, the Digital Markets Act and the Cybersecurity Strategy, the European vision for Digital EU by 2030 based on the principles of digital inclusion has become a priority as existing problems such as digital divide and cyberattacks have increased as it is also seen in ENISA's Threat Landscape Reports (COM, 2021).

A positive regulatory development is the Network and Information Security Directive which aims to establish a common level of security for network and information systems that play a vital role in the society by addressing the threats posed to those systems. The Network and Information Security (NIS2) Directive places measures and requirements on cybersecurity and resilience in EU member states. The NIS2 expands the scope of application and covers 'essential services' including, postal and courier services, and measures that will need to be taken at a much larger scale across the continent. Member States must comply with NIS2 Directive until October 2024 and adapt to the challenges. Postal service providers, as indicated in Directive (EU) 97/67/EC, is demonstrated in Directive (EU) 2022/2555. Providers include courier services and are subject to the Directive if they conduct any of the following activities within the postal delivery chain: clearance, sorting, transportation, distribution of postal items and pick-up services. The degree of dependency on network and information systems is also taken into consideration (Directive EU, 2022).

Digitalisation is changing supply chains and the way people buy online. The upward trend of e-commerce (European Commission, 2022a, 2022b) has created numerous challenges for the EU postal sector stemming from the new needs that emerged at a different rate in each member state, making it difficult to apply harmonised administrative practices. Consequently, there are many debates as to whether the current regulatory framework needs revision as member states are transforming at a different pace, making it impossible to apply a one-size-fits all solution.

The pandemic era accelerated the need for further digitalisation of the postal sector and gave space to the development of new technological tools on behalf of the postal enterprises that for the first time aim primarily to the end-user. Pandemic also demonstrated emphatically the utmost need for further protection of the postal chain process that becomes more digitalised and at the same time gave way to the development of new more digitalised and secure last mile services that will cover the end-users needs.

Furthermore, other developments such as the use of smart box open networks or the use of autonomous drones which are planned to be used by many companies to make mail delivery easier for postal deliveries in rural or secluded regions of the EU is another critical step that is mean to be applied. Last mile delivery and sorting and logistics use the latest technologies to address the demanding environment that the pandemic era created. Digital platforms that cannot operate separately from the postal and courier sector are changing infinitely the commercial habits of the end-users. Like any other new technology, there need to be guidelines around safety and privacy that should be addressed aiming to protect the end-user's civil rights and at the same time to balance with the rules of postal and courier market.

Digitisation as well as new and improved services via advanced technological developments has changed the role of the postal sector. The advances in ICTs create new opportunities and demands for the postal market. Operators who are not digitised have the risk of being excluded. Consequently, it is essential to develop a culture of security founded on the principles of confidentiality and privacy from the first mile to the last mile and every step in between, since privacy and confidentiality are perceived as major quality indicators.

6 Compliance with technical standards

Standards are of the utmost importance in the postal industry as they guarantee effectiveness, dependability, and client contentment. The standards in question cover a wide range of postal operations, encompassing delivery, security, international cooperation, and correspondence management. Health and safety, universal service obligations, quality of service, security and confidentiality, international mail exchange, technology and digitalisation, environmental sustainability, and international mail exchange are all critical areas in which standards play a pivotal role. The different postal traditions and cultures in Europe make the establishment of a common and unified set of rules a difficult procedure. Thus, a set of requirements as defined by the standards is crucial. A standard is established by consensus and is approved by a recognised body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in each context.

The European Commission has promoted and supported the creation of technical standards in the postal sector. Postal service directives identify the role standardisation plays in benefiting postal customers and operators. European postal standardisation aims on key priority areas to achieve harmonisation of technical methods at EU level. Developing measurable standards for the postal sector contributes to the protection of postal employees and postal items. In addition, contribute to the protection of the overall postal supply chain. The UPU Convention states, in Article 8, that member countries and their designated operators shall observe the security requirements defined in UPU security standards as well as adopt and implement a proactive security strategy at all levels of postal operations. Furthermore, the requirements set by the International Organization for Standardization are generic and intended to be applicable to all organisations. For instance, the International Standard ISO/IEC 27002:2022 'Information security, cybersecurity and privacy protection Information security controls' is designed as a reference for selecting controls within the process of implementing an information management system (IMS) or as a guidance document for organisations implementing

commonly accepted information security controls. It is essential that an organisation follows a management framework which initiates and controls the implementation and operation of information business requirements and relevant laws and regulations.

Furthermore, it is critical to establish security within the organisation and protect confidentiality, authenticity and/or integrity of information. Within this context employees and contractors should be aware of their responsibility to report information security events. Situations to be considered for information security event reporting include ineffective security control, breach of information integrity, confidentiality or availability expectations, human errors, non-compliance with policies or guidelines, breaches of physical security arrangements, uncontrolled system changes, malfunctions of software or hardware, access violations. Another factor that ought to be considered is that secure information system engineering procedures based on security engineering principles may be applied to in-house information system engineering activities and be regularly reviewed. A consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses ought to be addressed. With due care of confidentiality aspects, information security incidents can be used in user awareness training as examples of what could happen on how to respond to such incidents.

Other standards which regard the adoption of a quality management system may help improve the overall performance and provide a sound basis for suitable development initiatives and help through effective preventative and protective measures to minimise risks. An enterprise in the postal sector can use a variety of methods to maintain its knowledge and understanding of its compliance status and may benefit via a systemic approach as regards the use of technical standards in this new technological era.

7 The importance of education in the postal and delivery sector

The decisive step that should be taken by all postal and courier operators is training employees according to the new demands and challenges of the new era respecting at the same time important human and civil rights such as privacy and confidentiality that add up to a high standard way of living.

In the first place the characteristics of the new changing postal sector environment must be defined. Nonetheless this new environment of digitalisation of the postal market that emerges is highly competitive and demanding and needs urgently services of high quality, in a multi-cultural environment and at the same time needs to be respectful of citizen's privacy rights. At this point postal providers must be flexible and should invest in training their employees in using the new digital technologies and must realise that evolving training programs and e-education are key factors not only for quality of services they provide, but also for the protection of the civil rights of privacy and confidentiality. For instance, the postal and courier enterprises should design an annual staff training plan, according to their needs, which will target to the staff's awareness about matters of privacy and confidentiality and digital skills in new technologies as described above. This will lead to the development of confidentiality and privacy aware staff culture inseparably connected to high quality postal and courier services. In addition, they must implement digital strategies, utilise all digital tools at their disposal,

and deploy digital solutions that satisfy e-commerce standards, as this is also emphasised and supported by UPU (Digital Readiness for E-Commerce, 2021).

Training tends to be a priority if the goal of the market is to meet the needs of the dawning new era. Employees ought to prioritise the development of their digital competencies. Additionally, they require training, for instance on delivery drones and sorting robotics. Furthermore, it is essential to receive training in data privacy, cybersecurity, and compliance with the existing regulatory framework. Privacy and confidentiality should acquire a most crucial role during any kind of postal training.

8 Conclusions

The rise of digital technology has created both threats and opportunities for the postal sector. The regulatory framework of the postal sector along with the courier and parcel market should receive broader definitions and must be perceived in a holistic view within the function of a fast changing and alternating environment.

Digital innovations, e-commerce, automatisation have become a strategic priority pushing its employees to follow the new digital era. In this new postal era, it is essential for post office employees to be able to adapt, learn new skills, instruments, or procedures. Soft skills such as adaptability and flexibility to the new changing environment are essential.

A systemic approach to postal security could be applied which would ensure safety, integrity, and reliability of postal services through the implementation of an all-encompassing and synchronised collection of procedures and measures. This approach acknowledges the comprehensive nature of postal security, which encompasses not only the protection of mail against theft, but also the infrastructure, personnel, and consumers of the postal network.

Furthermore, what should be stressed out from a regulatory perspective is that policy intervention needs careful consideration. It is often the case that regulatory failures may occur when competent authorities try to impose measures in a horizontal way. The e-commerce market is a dynamic sector, and a dynamic assessment is essential as regards the current regulatory framework. Otherwise, there is a high likelihood that the regulation is outdated and unsuccessful regarding the initial purpose it is created for. Digitisation has influenced postal enterprises and consequently postal sector security and security planning is essential. Furthermore, suitably trained postal staff may lead towards an intended security outcome.

Associated protective measures, response planning and training of staff can lead towards secure organisations. Furthermore, effective rules ought to be explored and adopted, based on the regulatory framework of each member state (ERGP Report, 2022). Collaboration among the competent authorities, exchange of best practices as well as consideration of the market momentum can benefit customers and lead towards a more secure postal and delivery sector.

References

ADAE (2021) Decision of the Board 160/12.05.2021, ADAE (2021) Decision of the Board 349/5.11.2021, ADAE (2022) Decision of the Board 20/10.02.2022.

COM (2021) *118 Final 2030 Digital Compass: The European way for the Digital Decade* [online] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.andENISA,ThreatLandscape2022 (accessed October 2022).

Digital Readiness for E-Commerce (2021) *UPU E-Commerce Guide, UPU Enablers for E-Commerce*.

Directive EU (2022) *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, 27 December.

ERGP Report (2022) *Developments in the Postal Sector and Implications for Regulation, March 2019 and ERGP Position Paper on the EC Report on the Application of the PSD*, ERGP, April.

European Commission (2022a) *Report/Study*, Digital Economy and Society Index (DESI) (DESI-Full European Analysis 28.07.2022).

European Commission (2022b) *Public Stakeholder Workshop on the Main Developments in the Postal Sector between 2017 and 2021, Copenhagen Economics*.

Hellenic Authority for Communication Security and Privacy (2005) *Regulation for the Assurance of Privacy in Postal Services [(GG No. 384/Issue B/24-3-2005 (Decision No. 1001)]*, Hellenic Authority for Communication Security and Privacy.

Lone, S. and Weltevreden, J.W.J. (2022) *European E-Commerce Report*, Amsterdam University of Applied Sciences and Ecommerce Europe, Amsterdam/Brussels.

Universal Postal Union (2019) *Convention Manual*, International Bureau of the Universal Postal Union, Berne.