UNIO - *EU Law Journal*. Vol. 10, No. 1, May 2024, pp. 16-29.

School of Law – University of Minho

Data protection and appropriate measures: too many uncertainties in the judicial applications?

Giovanni Maria Riccio*

ABSTRACT: The present paper analyses, from a comparative perspective, the accountability rules outlined in the GDPR and their practical application by the courts of Member States. The first part of the article highlights the influence of the GDPR on Third Countries, with specific attention to Chinese legislation regarding data protection. The second part is mainly focused on the obligations relating to accountability and the notion of appropriateness of measures to be adopted by Data Controllers, as well as its connection with liability rules stated in Article 82 of the GDPR. The analysis considers the application of these rules, emphasising the different interpretations made by Data Protection Authorities, national courts, and more recently, by the Court of Justice of the European Union.

KEYWORDS: Data protection – accountability – appropriate measures – liability – comparative law.

* Full Professor of Comparative Law, University of Salerno, Italy.

1. Introduction

It is well known that the Regulation (EU) 2016/679 (GDPR) has profoundly innovated and modified the foundations on which the legal framework for the protection of personal data was based. The approach, which includes principles such as accountability and self-responsibility, appears significantly renewed; the obligations on the Data Controller are not typified (in the sense that they are not expressly listed), but the GDPR leaves the controller to take the choices concerning the data protection measures to be adopted.[1]

Many rules of the GDPR use generic formulas, often not defined, which, while on one hand demonstrate flexibility, on the other hand raise doubts about the actual measures to be adopted, leaving ample discretion to supervisory authorities (i.e., the Data Protection Authorities or DPAs).

European law, starting from the early Directives on consumer law,[2] has often been based on two specular principles. On one hand, the protection of vulnerable (or weak) parties, such as the consumer and, in the GDPR, the data subject. This protection is ensured through balancing informational asymmetries, and making individuals informed about the use and purposes for which their data will be used. On the other hand, according to the economic analysis of law, compliance costs are transaction costs that, if borne by data controllers, should avoid sanctions. However, the legislative framework of the GDPR leaves many uncertainties and as already mentioned, allows supervisory authorities to sanction violations that may be vague and abstract.

The present paper is divided into two parts. The first part will analyse some non-European legal models that have imitated the GDPR, adopting many similar formulas and referring to the principle of accountability, and to the obligation to adopt security measures. In the second part, the scope of application of security measures and their impact on both administrative and non-contractual liability will be analysed.

2. GDPR and legal transplants

The accountability principle is one of the cornerstones that has been widely reproduced in non-European countries after the entering into force of the GDPR.

For example, the Brazilian law [(Law No. 13.709 of 2010, also known as the *Lei General da Proteção de Dados* (LGPD)] has strong similarities to the GDPR;[3] for instance, it applies to natural or legal persons, public or private, collecting or processing personal data within the national territory or individuals located within the national territory, regardless of the location of the establishment; it mandates providing clear and comprehensive information to data subjects; it requires conducting impact assessments in cases of potentially risky processing, as well as maintaining a record of data processing activities.[4]

---

[1] On these aspects, see Alessandro Mantelero, "The future of data protection: Gold standard vs. global standard", *Computer Law & Security Report*, vol. 40 (2020): 1.

[2] Oliver E. Williamson, "Legal implications of Imperfect Information in Consumer Markets: Comment", *Journal of Institutional and Theoretical Economics*, vol. 151, no. 1 (1995): 49; and more recently Antonios Karampatzos and Nikol Ili, "Law and Economics of the Withdrawal Right in EU Consumer Law", *Review of Law & Economics*, vol. 19, no. 3 (2023): 435.

[3] See Ana Luiza Liz dos Santos, "Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais", *Revista dos Tribunais* (2020): 105.

[4] For further details, see Mario Viola – Leonaro Heringer, "Um olhar internacional: Lei Geral de

Pursuant to Article 50 LGPD, data processors and data controllers may elaborate, individually or through associations, rules of good practices and governance, as well as internal mechanisms for supervision and risk mitigation and most notably, security and technical standards.[5] On this aspect, the LGPD and the GDPR differ, in the sense that the latter admits the possibility of creating codes of conduct, but states nothing about determining common technical and security standards, leaving operators in a state of uncertainty that will be discussed further in this article. These rules of good practice and governance, at least in our opinion, are slightly different from certifications stated in Article 42 of the GDPR, in the sense that, from a formal point of view, they are not expected to be approved by any public authorities. However, the practical effect, that of determining a common standard, is similarly achieved.

Furthermore, in the Brazilian experience, the privacy governance should take into account the establishment of appropriate policies and safeguards based on a systematic assessment process of privacy impacts and risks, which is proportionate to the structure, scale, and volume of its operations, as well as to the sensitivity of the processed data. As well as the GDPR, Article 50 of the LGPD requires the data controller to demonstrate the adequacy of the measures adopted; however, the fact that there is a list of the minimal measures to be implemented undoubtedly makes compliance easier, at least formally, for Brazilian companies and public administrations compared to European ones.

A similar analysis could be made for the Swiss law, which came into force in 2020 after a lengthy legislative process that began in 2017.

Starting from the scope of application, the data of legal entities will no longer fall within the scope of personal data regulations. As in Brazil, the data controller will be required to adopt and maintain a record of processing activities; an impact assessment must be conducted in cases of processing with particular risks; the data controller must report any personal data breaches to the supervisory authority (*Préposé fédéral à la protection des données et à la transparence*).

It is also envisaged that the data controller appoints a representative in Switzerland in the case of companies established outside national borders. Regarding the rights of data subjects, the new text introduces, along the lines of the GDPR, the right to data portability, as well as the right not to be subject to a decision based solely on automated processing.

The new Swiss law also requires the data controller to adhere to the principles of privacy by design and privacy by default, and to ensure data minimisation in processing. Finally, the powers of the supervisory authority have been expanded, enabling it to conduct inspections and issue binding decisions.[6]

Many other countries have adopted regulations modelled on the GDPR, such as the Nigeria Data Protection Regulation (NDPR), issued in January 2019 and the Egyptian Law No. 151 of 2020. Undoubtedly, the choice of smaller countries reflects

---

Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados", in *Lei Geral de Proteção de Dados (LGPD): caderno especial*, ed. Carlos Affonso Souza, Eduardo Magrani and Priscilla Silva (São Paulo: Thomson Reuter, 2019), 227.

[5] Bruno Dantas and Leonardo Rigotti de Ávila e Silva, "Risco, compliance e proteção de dados", in *Compliance e Políticas de Proteção de Dados*, ed. Ana Frazão and Ricardo Villas Bôas Cueva (São Paulo: Thomson Reuters Brasil, 2021), 301.

[6] Philippe Meier and Sylvain Métille, *Loi fédérale sur la protection des données* (Helbing Lichtenhahn Verlag), 2023.

the need to facilitate commercial relations with Europe, beyond the undeniable legal prestige that the GDPR has gained. Similarly, the choice to emulate the GDPR is almost obligatory for Switzerland, being geographically European, albeit not a part of the European Union (EU). However, it is surprising that similar principles are adopted by an "economic giant" like Brazil.

A separate discussion, however, must be had – albeit briefly – regarding the data protection reform in China. The so-called PIPL – "*Personal Information Protection Law*" – came into force on November 1, 2021, after a long legislative debate. It is probably a fundamental step in a globalised economy, considering that the Chinese legal system has followed some of the EU legislative choices, mirroring many of the provisions found in the GDPR.[7]

First and foremost, the scope of application of the new regulation encompasses three main scenarios: a) processing activities conducted within Chinese territory; b) provision of products or services to Chinese citizens or analysis of their behaviours; c) all other cases provided for by national special laws. In cases where an entity established outside Chinese territory processes personal data falling within the scope of the PIPL, then, according to Article 53, it will be required to have an establishment in China or designate a representative, reporting the name and contact information of the latter to the competent authority. Another similarity with the GDPR is found in Article 72 of the PIPL, which specifies that the Chinese law does not apply to personal data processing carried out by individuals for personal or household reasons.

Similarly, the PIPL follows the division between data controller and data processor, identifying the relevant figures based on the framework outlined by the GDPR: thus, the controller is the one who determines the purposes and means of processing, while the processor acts within a model akin to an agency relationship, following the instructions of the controller.[8] Strong analogies can be also found in the information – comparable to those listed in Article 13 of the GDPR – that must be provided to the data subject at the time of data collection.

The regulation of data concerning religious beliefs and health status is similar, although, unlike the European legal model, financial data and, in general, the financial status of an individual also fall under the category of sensitive data. With a significant provision, considering recent controversies involving the Chinese government, biometric information is also considered sensitive data. Additionally, data concerning minors under the age of fourteen are subject to specific protection measures, as is the geolocation information of the data subjects.

Finally, the various legal bases legitimising data processing sometimes closely resemble those enumerated in the GDPR. First and foremost is consent, which, identical to Europe, must be freely given, specific, and revocable, as stipulated in Article 14 of the PIPL.[9] Such consent – another analogy with the GDPR – is not required if the data are necessary for the conclusion or performance of a contract

[7] See Corrado Moriconi, "Recent evolution of the personal privacy legal protection in People's Republic of China", *Nordic Journal of Law and Social Research*, vol. 9 (2019): 248; Giulio Santoni, "Personal data as a market commodity: legal irritants from China "experience", *European Journal of Privacy Law and Technology*, vol. 1, (2023): 1.

[8] Rogier Creemers, "China's Emerging Data Protection Framework", November 16, 2021, available at SSRN: https://ssrn.com/abstract=3964684.

[9] Igor Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)", *Smart Cities*, vol. 5 (2022): 1140.

or to fulfil a legal obligation. Similarities can be found in the provision legitimising data processing in case of public health emergencies or to protect the life, health, or property of an individual, always in the event of a health emergency.

Regarding the assessment measures, Chinese law appears heavily focused on the issue of data transfer. This choice is not surprising, considering that China has made a deliberate political decision in the legal imitation of the GDPR: a legal imitation not based on the prestige of the European legal model, but mostly on commercial needs. Therefore, when data is exported from China, special attention is required. Another possible interpretation could be the Chinese government's concern that data is transmitted outside the national territory. However, it should not be forgotten that the PIPL contains specific provisions regarding information concerning China's national security and public interest, and other regulations strictly protect trade secrets.

Data transfer is regulated by Chapter III of the PIPL, which requires an assessment[10] before personal information exportation, is similar to the Data Protection Impact Assessments (DPIA) as regulated by the GDPR, albeit with some additional requirements.[11]

The assessment process should be focused on the following aspects. First, an evaluation of the validity, necessity, and appropriateness of the data transfer, and it also has to be conducted through a specific assessment on the scope, category, and sensitivity of the data. Furthermore, it is required that the overseas recipient has robust organisational and technical measures to safeguard against data loss or damage, also identifying risks associated with data tampering, destruction, leakage, loss, transfer, or unauthorised acquisition or use during or after export.[12]

It is important to underline that Article 40 holds that the assessment must be approved by the State's cybersecurity and informatisation department and is mainly based on security issues. Furthermore, this obligation is provided for in the event that operators of critical information infrastructure and personal information handlers reach quantities provided by the same department.

Therefore, the primary difference between the Chinese and European legal frameworks lies in the entity responsible for conducting the assessment. In China, a private self-assessment is not permitted, and it must be "*validated*" by a public authority, thus adhering to uniform standards. Conversely, under the GDPR, the measures adopted are not predetermined, and the data controller can choose any option deemed adequate to protect data security. In this sense, the Chinese system

[10] Article 38 of the PIPL holds four different and alternative criteria: "a) Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law; b) Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department; c) Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides; d) Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department". The translation of the PIPL is made by Rogier Creemers and Graham Webster on the basis of DigiChina's earlier translation of the of the second review draft of the law and is available here: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[11] Guan Zheng, "Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China", *Computer Law Security Rev.*, vol. 43 (2021): 105610.

[12] W. Gregory Voss and Emmanuel Pernot-Leplay, "China Data Flows and Power in the Era of Chinese Big Tech", *Northwestern Journal of International Law & Business*, vol. 44, (2024): 1.

presents, at least formally, fewer uncertainties compared to the EU's system. The flip side, of course, is constant state monitoring of data flow.

The path of analogies and similarities between the PIPL and the GDPR strongly diverges, however, when transitioning from private relationships to those of public law, particularly in the relationships between the State and citizens. It could be said that the PIPL is divided into two branches. The first is oriented towards commercial relations with Europe (and, generally, with third countries), reflecting many regulatory provisions of the GDPR. The second, on the other hand, concerns public law and, in this sector, the distance between the two legal models remains sharp.[13]

For instance, a rather extensive sub-category of sensitive data concerns information that, if unlawfully disclosed, could cause harm to individuals' dignity, national security, or property: perhaps an excessively broad definition, reflecting an imbalance between individuals and political power. A separate case, not found in EU legislation, concerns processing for journalistic purposes, political reasons, or otherwise for a purpose of public interest.

Furthermore, the PIPL does not play a central role in the Chinese IT Law ecosystem, as the GDPR does in Europe. The PIPL, in fact, is part of a broader regulatory framework where cybersecurity takes a leading role, and within a legal system where, concerning fundamental rights, the protection of personal data still plays a secondary role.[14]

3. Security measures and accountability principle

As mentioned, the GDPR includes accountability among its fundamental principles. As briefly mentioned, this is a regulatory model followed in many non-European legal systems, which, however, in terms of practical application, may give rise to numerous hermeneutic issues.

Indeed, the previous legislation held obligations with standardised requirements that the data controller had to adhere to, including a series of necessary minimum measures. Today, on the contrary, the GDPR allows the data controller the freedom to select the tools by which to prevent a qualified personal data breach, defined in Article 4(12) of the GDPR as an event that accidentally or unlawfully leads to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed. The provision thus covers both deliberate attacks (e.g., malware, computer viruses, etc.) originating from third parties and instances where such occurrences result from negligent, albeit accidental, conduct by the data controller. For example, this could include the unauthorised transmission of a database to an unauthorised recipient or the loss of a hard disk containing personal data.

The remedy for a data breach is regulated by Article 32 of the GDPR, which states that the data controller must notify the competent supervisory authority of the personal data breach as soon as possible and, in any case, within 72 hours of becoming aware of the incident. However, such notification is not required in every

[13] For further details on this aspect, see Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Flaw: A Third Way Between the US and the EU?", *Penn State Journal of Law & International Affairs*, v. 49, no. 8 (2020): 49, according to whom China is a third way if compared to the American and European approach to data protection.

[14] For a comprehensive examination of Chinese regulations, see Giulio Santoni, *note* 7.

case, but only when the breach poses a risk to the rights and freedoms of individuals. The assessment is left, in line with the principle of self-responsibility mentioned earlier, to the data controller, as the choice of the actual technical measures to be adopted in case of data-breach to minimise the risks connected to the event.

However, analysing the wording of Recital 74, Article 24, and Article 32 of the GDPR, some nuances arise. According to Recital 74 of the GDPR, the data controller should implement appropriate and effective measures, and be able to demonstrate compliance with this Regulation, including the effectiveness of the measures, and such measures should take into account the nature, scope, context, and purposes of the processing, as well as the risk to the rights and freedoms of individuals. Article 24 of the GDPR adopts the same parameters as Recital 74 (nature, scope, context, purposes of processing), but concerning risks, it refers to those with varying likelihood and severity for the rights and freedoms of individuals. Lastly, Article 32 of the GDPR, while echoing again the same parameters as the aforementioned rules and using the risk parameter mentioned in Article 25 of the GDPR, sets out in a different way, noting that the measures to be taken to demonstrate compliance with the obligations of the Regulation must also take into account the state of the art and implementation costs.

However, reflecting on the slight differences among the three regulations, a doubt arises. Should the responsibility of the data controller, in the case of adoption of inadequate security measures, be interpreted according to subjective or objective parameters? Is the data controller liable if it has not adopted protective tools available on the market, but deemed excessively costly based on their own economic resources? Or should an objective criterion be followed, prioritising the assessment of risks associated with the specific data processed or, probabilistically, the likelihood that the data controller will be subjected to abusive attempts of unauthorised access (e.g. public bodies or hospitals managing millions of sensitive data)?

This point is further analysed in the following pages of this paper, but it demonstrates the uncertainty and is one of the major issues related to the practical implementation of the rules of the GDPR.

For instance, the adoption of privacy by design and privacy by default measures is not compulsory and these measures are not legislatively defined; however, there have been cases where supervisory authorities have imposed sanctions for the failure to adopt a privacy by design plan in identifying security measures. How should this be considered? Is it a legal obligation or it should be considered on a case-by-case approach, bearing in mind, on the one hand, the seizure of the data controller and, on the other, the nature of the personal data processed, and the risks associated to them? Again, this ambiguity is allocated on the data controllers (i.e., on private companies and public administrations), and the practical application of the rules is committed to the national DPAS, whose interpretation could also be different from one country to another.

Too often, it is forgotten that the objectives of the GDPR are listed in Recital 2 of the Regulation, where it is stated that "*This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons*" as well as in Recital 13, where it is stated that "*In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation*

is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States".

Therefore, even in the application of the rules, there should not be differences between individual DPAs, considering two aspects. The first is that there is a body, the European Data Protection Board (EDPB), which, among other things, has the task of ensuring uniformity in the application of the rules. The second is that DPAs, under the GDPR, have changed their nature, becoming supervisory authorities without the power to create legal rules.[15]

Furthermore, it must be considered that DPAs are public and administrative bodies and, according to Article 51 GDPR, independent public authorities. This means that DPAs' decisions must be motivated and held within a specific time, as for all the acts held by public authorities.

As public authorities, their provisions (such as those applying fines or sanctions to the data controllers) must be substantiated, and a lack of a proper statement of reasons may lead to the annulment or to the overturning of these provisions. Then, in case of fines based on the violations of Article 32, the infringed measures should be indicated/listed under the provision on fines and sanctions.

A recent decision held by the Court of Milan in October 2023 annulled a fine imposed by the Italian Data Protection Authority because of the vagueness of the motivation of the DPA's provision. In fact, this provision contested the lack of the adoption of security measures, notably those concerning organisational measures aimed at improving the data subjects' rights, plus the scarcity of references to precise pieces of evidence to support the evaluation of the amount of the fine.

Similar conclusions were also held in Poland by the Supreme Administrative Court[16] and by the Administrative Court Warsaw.[17] The decision concerned the alleged failure of Morele.net (an online retailer) to fulfil its obligation to implement sufficient data security measures, which could have facilitated a phishing attack resulting in the unauthorised acquisition of a customer database, thereby breaching GDPR obligations concerning the assurance of data security and integrity.

In this case, the Supreme Administrative Court invalidated the decision of the Polish DPA as well as the judgment of the Voivodeship Administrative Court, which had confirmed the fines imposed by the privacy authority. According to the decision, Article 32 GPDR underscores that administrative sanctions are not imposed solely for unauthorised personal data processing, but rather for failing to maintain an appropriate security standard given the circumstances. In essence, entities are not held accountable for malicious actions by third parties, such as hacking, but rather for inadequate security measures that may have facilitated such breaches. Therefore, mere unauthorised data access does not necessarily violate Article 32 GPDR, as even the most robust security can potentially be compromised.

The decision also recalls the Recital 76 GPDR, emphasising the need for an objective assessment of risk levels associated with processing operations. Consequently, the "*appropriate*" measures mentioned in Article 32(1) are not judged by their absolute

[15] See on this aspect: Administrative Court of Rome, 15 January 2023, no. 603/2023.
[16] February 2023; III OSK 3945/21.
[17] October 2022; II SA/Wa 567/22.

effectiveness but rather, by their relevance to the specific situation and timing of data access.

According to the Court, the Polish DPA should have granted the company's request for the appointment of an external expert, that would have been responsible for examining the technical measures implemented by the company itself to safeguard its data. Additionally, the expert's role would involve assessing whether the adopted precautions were proportionate to the recognised risks within the e-commerce sector.

Also, a Hungarian case is worthy of mention in this context. In November 2021, the Hungarian Supreme Court stated that the DPA cannot levy fines in proceedings if it significantly surpasses the statutory time limit set for its own procedures.

It is necessary to point out that the regulations of the single national authorities establish procedural deadlines within their respective procedures. Generally, these deadlines are not considered binding. Therefore, the Hungarian decision is interesting because it cancelled the sanction imposed by the national DPA, considering the deadlines to be strict and requiring adherence. In this specific case, the proceedings started on 19 November 2018, and the DPA issued its final decision on 15 July 2020.

4. Court of Justice and security measures

Once we have examined the framework of case law from individual Member States regarding compliance obligations and the powers of DPAs, the application of the GDPR by the European courts seems similarly challenging.

The Court of Justice of the European Union (CJEU) has recently returned to address issues regarding personal data protection and liability with a ruling that is generating an extensive debate. It is indeed the first time Luxembourg judges have taken a stance on the relationship between security measures and immaterial damages (regulated by Article 82 GDPR), resulting from personal data breaches.

The preliminary question arose from a dispute between a Bulgarian citizen and the National Revenue Agency of that Member State (NAP), linked to the Ministry of Finance. NAP, during 2019, suffered a hacker attack involving unauthorised access to the agency's computer systems, theft, and subsequent publication of personal data stored within these systems on the internet.

The cyberattack affected a vast amount of data, concerning approximately six million users, some of whom lodged complaints with national authorities seeking compensation for non-material damages arising from fear that their personal data, published without their consent, might be subject to future misuse, or that they might become victims of blackmail, assault, or even kidnapping.

The NAP stated that it had implemented all necessary measures, as prescribed by Article 32 GDPR, to prevent the breach of personal data it held and, following the breach, had taken all necessary measures to minimise the effects of that breach, aiming at protecting the rights and freedoms of the data subjects, namely the individuals whose data had been compromised.

At first instance, the Administrative Court of Sofia (*Administrativen sad Sofia-grad*) dismissed the compensation claims, ruling that the NAP had taken adequate measures to prevent unauthorised access to its computer systems and the theft of personal data, and that the claimant had not demonstrated the damage suffered or the causal link between the event and the damage.

The losing party appealed the decision to the Bulgarian Supreme Administrative Court (*Varhoven administrativen sad*), arguing that the first instance judge had not

correctly assessed the burden of proof. Thus, NAP should have to demonstrate the use of effective security measures and that the fear of unlawful use of personal data was real and current, not merely hypothetical.

The referring judges thus addressed the following questions to the CJEU. Firstly, whether a national judge is competent to assess the adequacy of security measures adopted and their ability to prevent damages resulting from a breach. More specifically, the question concerns the possible existence of an automatism, i.e., whether the unauthorised disclosure of personal data following a data breach event is sufficient to determine that the technical and organisational measures adopted are inadequate to protect the rights of data subjects. Secondly, the issue concerning the burden of proof, and whether the demonstration of the adequacy of technical and organisational measures by the data controller rests on the controller or on the party claiming to have suffered damage. Similarly, whether the fact that the harmful event is attributable to third parties exempts the data controller from liability.

Finally, and perhaps the most interesting aspect, the last preliminary question asks the CJEU whether compensation for non-material damages may be granted for mere concerns and anxieties and mere fears experienced by the data subject regarding potential future misuse of personal data, even if further damage has not been demonstrated on the part of the claimant.

The CJEU – correctly, albeit not surprisingly – emphasises that the mere verification of a violation is not in itself sufficient to trigger liability on the part of the controller. Indeed, a different conclusion would have been incompatible with the wording of Article 24 GDPR, which explains that the adequacy of the processing measures implemented by the controller is necessary not only to ensure effective protection of the rights and freedoms of data subjects but also to demonstrate – by the controller itself – a diligent behaviour and, therefore, not to be held responsible for the detrimental effects of the data breach.

However, nothing is added about the obligations of the controller in relation to the adequacy of the measures. It could be an issue because some entities – such as public bodies, as in the present case – are burdened with significant costs for data security and organisational measures, and, in general, for the implementation of adequate protection measures, while facing an endemic scarcity of economic resources.

It should be made clear: it is not asserted that negative economic contingencies can justify the adoption of inefficient systems, but solely that, in the Court's interpretation, the only aspect that seems to be recurring is that of the obligation to ensure that all precautions are taken to ensure (and, in the event of a breach, demonstrate) compliance with the Regulation's obligations. Any consideration given to whether the cost of such protection measures, if excessive, can be taken into account as a parameter for assessing the controller's diligence obligations.

Thus, in the CJEU's interpretation, any economic difficulties of the controller, especially when related to the nature of the data, purposes, and context, cannot be considered as mitigating factors and exempt the controller from liability. In the judgment, however, specific risks associated with the processing must be taken into account: in the case of a public entity processing the data of millions of citizens, the judgment rightly focuses exclusively on assessing the conduct specific to the type of processing, as well as the nature of the controller and its exposure to risk (indeed, central bodies of public administrations are frequently targeted by attempted cyber-attacks).

The further question posed to the Court, relating to the burden of proof and, therefore, the circumstance that it is the controller who must provide evidence that all necessary measures to prevent data breaches have been taken, is more complex.

In fact, from Articles 5, 24, and 32 GDPR, the burden of proof lies with the controller. This is evident from the fact that, respectively, the first mentioned provision states that the controller is responsible for complying with the principles of the Regulation, and must be able to demonstrate compliance with those principles, while the other two provisions, with identical wording, provide that the controller must prove that sufficient technical and organisational measures are in place. Furthermore, as correctly noted by the decision, this conclusion is also derived from the "*architecture*" of the Regulation, which, as already mentioned, allows the controller to choose how to ensure the security of the data, without imposing specific obligations to be met.

Less straightforward, however, is the further sub-question, in which Luxembourg judges are called upon to rule on the need for judicial expertise as a systematically necessity, and sufficient proof to demonstrate the negligence of the controller. Such a provision, if strictly required, would align with the Union principle of effectiveness because, while respecting the procedural freedom of individual Member States, modalities of proof that make it impossible or, in any case, complicate the exercise of the rights recognised by European legislation cannot be required – especially in the absence, as in the Regulation, of specific indications.[18]

5. Compliance measures and liability of the data processor

Then, the judgment deals with the matter of tort liability arising from unlawful processing of personal data. On this aspect, it is useful to make a quick digression on the applicable regulations and legislative policy choices being the legislative option of Article 82 GDPR. Article 82 GDPR substantially mirrors Article 23 of Directive 46/95/EC, adopting a no-fault liability standard, retaining a negligent element in the specific case.[19]

---

[18] On this principle, see Norbert Reich, "The Principle of Effectiveness", in *General Principles of EU Civil Law* (Intersentia, 2013), 89.

[19] This issue of the national differences in tort law is complex and can be only briefly mentioned in this paper. The first key point of the debate concerns the nature of liability. In this sense, as has been pointed out, «the modern evolution of tort law shows a long-term tendency to distance tort law from the stance that moral or religious wrongdoing is, by itself, enough to establish civil liability» (Principles of European Tort Law (PETL), elaborated by the European Group on Tort Law. http://www.egtl.org). In the long term, we are witnessing a shift from a notion of "personal" liability to a more "functional/utilitarian" notion. If indeed, on the one side, personal responsibility remains a key concept in the discourse over the structure of tort law», still «the advent of vicarious liability, strict liability and the diffusion of no-fault, collective compensation schemes (...) have surely cast doubts on the meaning of the notion». Inevitably, the starting point for describing this evolution consists in the analysis of three main legal systems: (i) the French open-list model; (ii) the German closed-list approach and (iii) the UK tort based set of rules. Under the first of the three models, adopted for the first time in France: «*Tout fait quelconquie homme, qui cause à autrui un dommage, oblige celui per la faut duquel il est arrive, à le réparer*» (Article 1382 of the Civil Code, for a more detailed discussion see Genèvieve Viney, «Les conditions de la responsabilité», in *Traité de droit civil*, ed. J. Ghestin (Paris, 1982), 10. In other words, a liability claim can be brought, subject to the proof of (i) the damage; (ii) the causal relationship and (iii) the fault of the defendant. A similar model was adopted in Italy where, in addition to the three mentioned elements, further evidence concerning the "injustice" of the damage had also to be submitted. Separately, according to the closed list system established in Germany under the BGB, protection had to be granted in a number of specific circumstances, all expressly listed by

This argument is confirmed by paragraph 3 of Article 82, which provides that the controller "*shall be exempt from liability […] if it proves that it is not in any way responsible for the event giving rise to the damage*". This formulation mirrors that of paragraph 2 of the aforementioned Article 23 of Directive 46/95/EC ("*The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage*"),[20] which led some Nation States, in transposing the provision into domestic law, to apply the rules regarding liability for hazardous activities.[21]

The Regulation has again provided, like the 1995 Directive, a principle favourable towards the injured parties, requiring a rigorous burden of proof anchored to the non-attributability in any way of the wrongful act. However, it must be clarified that unlawful processing of personal data does not automatically entail a right to compensation, since, as specified, for instance, by Italian Court of Cassation, which stated that the damage (material and/or non-material) must be "*proved according to ordinary rules, regardless of its extent and the difficulty of fulfilling the burden of proof, as it concerns a consequential and not an event damag*e". Therefore, the mere violation of the GDPR rules, in the absence of demonstration of actual harm, is sufficient to justify an administrative sanction, provided the prerequisites are met, but not compensation for damages.[22]

However, there does not seem to be convergence between national and community case-law on the extent of the damage. Italian jurisprudence has argued that non-pecuniary damages can be compensated only in case of a significant harm, asserting that such damage is not exempt from assessment of the severity of the injury and the seriousness of the damage, thus balancing with the principle of solidarity derived from Article 2 of the Italian Constitution.

However, a recent judgment of the Italian Court of Cassation has departed from this approach, affirming that, in the matter of personal data processing, the injured party "*may obtain compensation for any damage suffered, even if the injury is marginal*".[23] Such a reading, in fact, aligns with a judgment of the CJEU, which similarly ruled that the right to compensation is not subject to the fact that the damage in question reaches a certain threshold of severity.[24]

---

the German codification. As for the elements to be proved, evidence had to be given also in relation to the (allegedly) "unlawful" nature of the act. Eventually, a totally different approach was adopted in the UK, where the original system for regulating liability was based on the "forms of action". Thus, in this context, there was not one single form of liability but, instead, a number of possible actions to be brought (torts). However, this hybrid scenario was not meant to remain unchanged. And in fact, over the time, the apparently strict borders among the three categories slowly shaded in the legal interpretation. More in detail, if on the one side under the French/Italian model, the notion of liability and recoverable damage was extended – and so it happened in the UK with the introduction of the tort of negligence –, on the other side the German closed-list model was subject to a broad interpretation, allowing to recover "the damage of any third party right". The described evolution, apart from reducing the distance among the three systems also contributed, in general terms, to the extension of the notion of recoverable damages and, specifically, to the adoption of a no-fault liability approach. For a general overview see Konrad Zweiger and Hein Kotz, *An introduction to Comparative Law* (Oxford: Oxford University Press, 1998).

[20] See Brendan Van Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", *JIPITEC*, vol. 7 (2016): 271, para 1.

[21] Such as Italian Law no. 675/1996, which applied Article 2050 Italian Civil Code regarding civil liability.

[22] See Italian Court of Cassation, 3 July 2014, no. 15240; 5 September 2014, no. 18812.

[23] Italian Court of Cassation, 12 May 2023, no. 13073.

[24] Judgment CJEU *Österreichische Post*, 4 May 2023, C300/21, ECLI:EU:C:2023:370.

Both decisions cited above refer to Recital 146 of the GDPR, where one can read that "*The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation*". Therefore, the qualification of damage could not have a national interpretation, as such an interpretation would undermine the harmonisation (i.e. unification) of European law on data protection.

However, the notion of damage – even from a comparative perspective – does not have a precise and sharp definition. Only the Austrian Civil Code has tried to provide a definition, albeit with a formula that has been interpretated differently by legal scholars.[25] Similarly, it is difficult to identify a clear explanation of the concept of damage within Union law, and sometimes, in its judgments, the CJEU has understood it as synonymous with injury.[26] Even the Directive on product liability, where damage also plays a fundamental role, does not help in this regard.

This means that, in general, the determination of the boundaries of the compensation of damage is still left to the discretion of national courts.

A parameter associated with the potentiality of harmful acts is difficult to be identified, unless it is intended, in relation to the case under consideration, to be identified solely in simple fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties. As the CJEU states, "*the wording of Article 82(1) of the GDPR does not rule out the possibility that the concept of 'non-material damage' in that provision encompasses a situation, such as that referred to by the referring court, in which the data subject invokes, in order to obtain compensation on the basis of that provision, the fear that his or her personal data will be misused by third parties as a result of the infringement of that regulation that has taken place*".

The judgment, therefore, disconnects the fact that such damage (which must still be proven) has resulted in a violation of the rights of the data subjects – necessary in the presence of material damages –, but goes on to consider that mere anxiety can be compensated. A different interpretation, indeed, "*would not be consistent with the guarantee of a high level of protection of natural persons with regard to the processing of personal data within the European Union*".

Considering this statement, the outcome of the decision could be disruptive and potentially lead to the collapse of companies and public entities affected by significant personal data breaches. Globally, from 2022 to 2023, the percentage of companies that have suffered data breaches exceeding $1 million has increased from 27% to 36%; establishing an automatism whereby the mere loss of control over data and the resulting fear of future damages could lead to compensation for the damage suffered, would undoubtedly distort the data protection regulatory system.

The weakness of the decision, in our opinion, lies precisely in its conclusions. In fact, although starting from the attempt to avoid discrepancies in the evaluation and quantification of compensation for damages by the judicial authorities of the individual Member States, the outcome is potentially antithetical, considering the vagueness of the notion of "fear".

Nevertheless, a possible interpretation of this notion could be found in some *obiter dicta* in the case-law of the European courts, from which it can be inferred that an identifying parameter of the damage should be found in its certainty.

[25] §1293 Allgemeines bürgerliches Gesetzbuch, ABGB.

[26] See Antoni Vaquer, "Damage", in *Tort Law of the European Community*, *Tort and Insurance Law*, vol. 23 ed. H. Koziol and R. Schulze (Wien: Springer, 2008), 30.

Although with non-uniform formulas, in the European case-law damage that must not only be real but also certain. Moreover, the Advocate General's Opinion in the latest precedent on the interpretation of Article 82 of the GDPR also considered that the European legislator, in other areas of Union law, has expressly provided for situations where the violation of a rule automatically results in the right to compensation: such scenarios must therefore be considered exhaustive, while in the case of the GDPR, it will still be necessary to have actually suffered damage.[27]

Therefore, starting from the assumption that, through security measures, the Regulation establishes a risk management regime and does not seek to eliminate the risks of personal data breaches at all, it must be concluded that non-pecuniary damage must be not merely potential, according to a subjective assessment of the presumed damaged party, but must in any case be real and certain. Therefore, non-pecuniary (or immaterial) damages resulting from a violation committed by third parties may give rise to compensation not if the data subject is afraid (which, as mentioned, could lead to frivolous mass tort litigation), but only if, based on probabilistic elements, the stolen data could actually be illicitly used (for example, for identity theft or computer fraud).

6. Conclusions

In the GDPR, out of 99 Articles and 373 Recitals, the word "*assessment*" recurs 47 times: it seems a huge number, but then we come across the proposal of the AI Act, out of 85 Articles and 89 Recitals, the same word appears 152 times, and in the Cyber Resilience Act, out of 57 Articles and 71 Recitals, 212 times.

Thus, the new regulations are continuously delegating the identification of their obligations' boundaries to their recipients, often resorting to non-legal norms (market standards, protocols, etc.).

Uncertainty is a risk to be avoided. In a ruling handed down by the Court of Milan last October, there was the suspension of a sanction of the Italian DPA because of its "*scarcity of references to precise elements*" of evidence and because of the "*generality of prescriptions on organizational and technical measures*".[28]

This is an important decision because it highlights that judges, accustomed to applying legal rules that provide clear obligations, struggle with the indeterminacy of accountability. Are we facing a clash between the "*formalistic technicalities*" of data protection, and those who are unaccustomed with the lexicon used by data protection experts and the meaning of sanctions, which are evidently too generic?

[27] Opinion of Advocate General Campos Sánchez-Bordona, 6 October 2022, C300/21, *Österreichische Post*, ECLI:EU:C:2022:756, para. 60.
[28] Court of Milan, 10 November 2023, no. 8858.