SHARING OF INFORMATION ON SERIOUS INCIDENTS (CHAPTER IX, SECTION 2) *

Olaya Fernández Fernández
PhD Candidate of Administrative Law
University of Oviedo

CONTENTS:

1. *Obliged parties*

The market surveillance authorities designated by each Member State shall be notified of serious incidents involving high-risk AI systems when the incident occurs within their territory. A serious incident is an 'incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

- the death of a person, or serious harm to a person's health
- a serious and irreversible disruption of the management or operation of critical infrastructure
- the infringement of obligations under Union law intended to protect fundamental rights
- serious harm to property or the environment'. [1]

The first paragraph Article 73 AIA expressly provides that this obligation is incumbent on the provider of an AI system, defined in the Regulation as a

* This paper has been written within the framework of the Research Project 'Algorithmic tools for citizens and public administrations', funded by the Spanish Ministry of Science and Innovation (PID2021-126881OB-I00).

[1] Article 3 (49) AIA.

'natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge'. [2] This obligation on the provider is also set out in Article 17 AIA, which stipulates a duty to establish a quality management system that systematically and in an orderly manner records documentation of policies, procedures and instructions on, inter alia, the serious incident reporting procedure of Article 73. [3]

From reading this first section, we can deduce the existence of a single obliged party: the provider, although, throughout the Regulation, there are other provisions that impose serious incident notification obligations on different parties, such as potential providers or deployers, which leads us to wonder whether there are more obliged parties.

The second and following paragraphs of the Article, concerning notification deadlines, stipulate that the maximum time limit for notifying a serious incident is a certain number of days (depending on the type of incident) after the provider *or, where applicable, the deployer*, [4] becomes aware of the incident, and gives both parties the right to submit the notification. In other words, the obligation to notify is solely and exclusively incumbent on the provider under the first paragraph, but the deadline depends on whether the provider or the deployer is aware of the incident, and both may submit the notification to the competent national authority. It is questionable what the legislator means by '*where applicable*' or how it is ensured that the notification will be made if the deployer does not notify the provider beforehand. It also raises doubts as to whether the deployer should be considered as an obliged subject, and there are arguments for a favourable but not conclusive answer, as will be discussed below. [5]

---

[2] Article 3 (3) AIA.

[3] Article 17 (1) (i) AIA.

[4] Article 3 (4) AIA defines the deployer as 'a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal, non-professional activity'.

[5] Professor Castilla Barea considers other arguments in favour but opts for a more restrictive interpretation of the rule: 'The latter could make sense in some cases if one considers its possible capacity to introduce substantial modifications in the AI systems it uses or because the use of the system itself may also entail risks.

In this regard, it is necessary to refer to Article 26 AIA, which sets out a series of technical and organisational measures that those deployers of a high-risk system must carry out. Among others, they must report serious incidents they detect, first to the provider, then to the importer or distributor, and finally to the market surveillance authority in the country where the incident occurs. Article 26 (5) AIA goes further and states: '[i]f the deployer is not able to reach the provider, Article 73 shall apply *mutatis mutandis*'. Whereby, if the deployer fails to contact the system provider, the deployer shall be obliged to report serious incidents under Article 73 (1) AIA, [6] which in our opinion constitutes a genuine subsidiary liability clause that will come into play when: a) there is both the provider and the deployer of an AI system [7] and b) the deployer, aware of a serious incident, is unable to contact the provider and assumes the notification obligation of Article 73.

On the other hand, the obligation to notify serious incidents is included in Chapter IX, which deals with the *ex post* control of these systems, and therefore refers to the obligation of the provider in the context of the marketing of a high-risk AI system; but the notification of incidents is an obligation that extends to other phases of the product's life cycle, such as the design and development of the system. Thus, Article 60 AIA lists a series of conditions and safeguards for providers (or potential providers) of high-risk AI systems listed in Annex III of the AIA to be able to carry out practices in real conditions, outside controlled test spaces (or AI regulatory

---

However, without other more secure and convincing arguments, we believe the decision should favour the more restrictive interpretation.'; Castilla Barea, M., *Vigilancia postcomercialización, códigos de conducta y directrices*, in Barrio Andres, M (dir.), *El Reglamento Europeo de Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2024, 155.

[6] The 'where appropriate' in 73(2) et seq. can be interpreted as referring to cases where the deployer, existing as a separate entity from the provider, is unable to contact the provider, whereby Article 73 applies *mutatis mutandis*: 'If the deployer is not able to reach the provider, Article 73 shall apply mutatis mutandis. This obligation shall not cover sensitive operational data of deployers of AI systems which are law enforcement authorities'.

[7] It should be noted that the figure of the deployer will 'not always exist' or at least not always separately from the provider of an AI system, as the provider is responsible for bringing the AI system to the EU market or putting it into service under its name or brand, while the deployer either acquires the system already on the market or develops and introduces it (in which case it will be both provider and deployer of the AI system).

sandboxes). Also, at this stage, providers or potential providers will be obliged to report serious incidents.[8]

The obligation to report incidents also applies to providers of general-purpose AI models with systemic risk, although in these cases, the reporting will be twofold. On the one hand, to the competent supervisory authority, but also to the AI Office, which will be informed of the serious incident and the measures proposed to remedy it.[9] Finally, the Board is responsible for collecting and preparing reports on serious incidents [Article 66 (e) (ii) AIA].

2. *Deadline for notification*

If the determination of the obliged party is not free of doubt, no less is to be said about the calculation of the time limits for carrying out the notification. The AI Regulation lays down a general time limit, in addition to which there are two special time limits.

The general deadline, i.e. the provider's obligation to report serious incidents occurring in the commercialisation phase of a high-risk system, shall be immediately after the provider (or, where applicable, the deployer) has established a causal link between the AI system and the serious incident, or when there is sufficient evidence to believe that such a causal link exists reasonably. In cases where the serious incident is clearly related to the operation of the AI system, the provider's obligation is immediate; whereas in cases where investigations are necessary to determine whether a causal link exists, the duty to report the incident arises as soon as there is a reasonable likelihood that this is the case.

In any case, the period shall be less than 15 days after the provider (or

[8] Article 60 (7) AIA: 'Any serious incident identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 73. The provider or prospective provider shall adopt immediate mitigation measures or, failing that, shall suspend the testing in real world conditions until such mitigation takes place, or otherwise terminate it. The provider or prospective provider shall establish a procedure for the prompt recall of the AI system upon such termination of the testing in real world conditions'.

[9] Article 55 (1) (c) AIA.

deployer) becomes aware of the serious incident.[10] This means that the protocols established by the providers will have to be sufficiently agile to try to clarify the causal link in a period of less than 15 days. In any case, this timeframe should be proportionate and consistent with the magnitude of the serious incident.

There are two considerations regarding this general time limit. First, if the provider is a figure other than the deployer and, moreover, it is the deployer who becomes aware of the serious incident, the general 15-day time limit starts to run from the time the provider (on whom the obligation to notify falls) becomes aware or from the time the deployer becomes aware. It seems logical to think, from an interpretation that safeguards the public interest, that the period starts to run from knowledge of the first of these. On the other hand, the reference to '[t]he period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident' is too ambiguous, without specifying whether the time limit should be longer or shorter the greater the magnitude of the incident.[11]

In addition to this general deadline, there are two special deadlines:

- In the event that the incident seriously and irreversibly affects the management or operation of critical infrastructure or is a widespread infringement,[12] the notification must be made immediately and, in

[10] The above-mentioned scenario of 26 (5) AIA may occur where the deployer becomes aware of a serious incident and then notifies the provider. In any case, it seems that regardless of when the provider becomes aware of it, the deadline for notifying the competent market surveillance authority will be 15 days from when the provider first becomes aware of it.

[11] In this sense, it may be thought that, given the magnitude of an incident, more time may be required to carry out the investigations, and therefore, the time required may be shorter or, on the contrary, the more serious the incident, the more urgency will be required in the communication.

[12] According to Article 3 (61) AIA, a widespread infringement is 'any act or omission contrary to Union law protecting the interest of individuals, which: (a) has harmed or is likely to harm the collective interests of individuals residing in at least two Member States other than the Member State in which: (i) the act or omission originated or took place; (ii) the provider concerned, or, where applicable, its authorised representative is located or established; or (iii) the deployer is established when the infringement is committed by the deployer; (b) has caused, causes or is likely to cause harm to the collective interests of individuals and has common

any case, within two days of the provider or deployer becoming aware of it.[13] As 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 (commonly known as the NIS2 Directive) establishes a notification procedure applicable to critical infrastructures and critical entities in terms of cybersecurity, this issue will be addressed below in section four to examine the compatibility of these rules of European Union law.

- In case of the death of a person, notification shall be made as soon as a causal link has been established (or there are reasonable grounds for suspicion) between the AI system and the incident, and in any case, within less than ten days after the incident becomes known to the provider or deployer.[14]

3. *Serious incident reporting procedure*

The provider or the deployer shall notify incidents immediately after the causal link has been established, and in any case, 15 days after the serious incident takes place (which, as we have seen, will be reduced to 10 days if the death of a person occurs, or to 2 days if the incident seriously and irreversibly affects the management or operation of a critical infrastructure). The notification shall be complete, although an incomplete notification (to be completed as soon as possible) is admissible where necessary to ensure that these deadlines are respected.[15]

---

features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States'.

[13] Article 73 (3) AIA.

[14] Article 73 (4) AIA.

[15] Again, the lack of clarity of the rule leads to the question of whether the general maximum time limit of 15 days (or the special ones of 10 and 2) applies with regard to the duty of complete or incomplete notification since Art. 73 (5) is silent on this: '[w]here necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report'. Although incomplete notification could be seen as an instrument to ensure that the maximum notification deadline is met, a more

Upon notification, necessary investigations shall be initiated in relation to the incident and the AI system, including a risk assessment of the incident and corrective actions. During the investigations, the provider shall cooperate with the competent authorities and, where appropriate, with the notified body concerned, but may not take any action that would modify the AI system in a way that could have an impact on an assessment of the causes of the incident, unless the competent authorities are informed in advance of such action.[16]

Where the serious incident has caused an infringement of obligations under European Union law aimed at protecting fundamental rights, the market surveillance authority shall inform the national public authorities or bodies designated by the Member States as responsible for monitoring or enforcing compliance with fundamental rights obligations under European Union law of the notification. This, in order to enable them to request any related documentation, where this is necessary for the effective fulfilment of their mandates within the meaning of Article 77 AIA.[17]

Within seven days of receipt of the notification, the market surveillance authority may take measures such as withdrawal or recall of the products or systems, including, where there is no other more effective means of eliminating the risk, a prohibition on the placing on the market of the AI system, in the same sense as set out in Article 19 of Regulation (EU) 2019/1020. When the market surveillance authority adopts any of the above decisions, it has a duty to communicate the measures taken to the Commission if it considers that the reasons for or effects of the measure go beyond the borders of the territory of its Member State, as well as the modification or withdrawal of such measures. It will also have to notify voluntary measures taken when the product presenting a serious risk has been placed on the market.[18]

---

public interest-friendly interpretation could also be chosen, whereby incomplete notification must be made as soon as the incident becomes known (in order to allow the market surveillance authority to take corrective action as it deems appropriate) and complete notification, including all information, must be made within the maximum deadline.

[16] Article 73 (6) AIA.

[17] Article 77 (1) AIA.

[18] Articles 19 and 20 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products.

In the case of a serious incident occurring at a pre-market stage, and in particular, at the live testing stage, market surveillance authorities may take a decision to suspend or terminate the testing in the real world or require the provider or potential provider and the deployer or potential deployer to modify any aspect of the testing in the real world. This shall be done through a reasoned decision, indicating how it can be challenged.[19]

4. *Exceptions to the notification obligation and relation to other EU law rules*

There are several legal acts of EU law that, like the AIA, include procedures for reporting incidents, security breaches or events that could affect the integrity of systems or the protection of fundamental rights. Among the most relevant rules provided for such procedures related to cybersecurity, privacy and data protection is Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. The Regulation establishes the reporting of major ICT-related incidents and voluntary notification of significant cyber threats. According to Article 19, financial institutions shall notify serious ICT-related incidents to the designated competent authority, and Member States may provide that some or all institutions shall also submit the initial notification and reports[20] to the competent authorities or the Computer Security Incident Response Teams (CSIRTs) designated in accordance with Directive (EU) 2022/2555.

Also, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or GDPR) establishes duties to notify the supervisory authority in the event of a breach of security of personal data (Article 33 GDPR). The controller's duty to notify the competent supervisory authority within 72 hours of security breaches that constitute a risk to the rights and freedoms of natural persons. This procedure, like that of the AIA, also allows for the practice of an incomplete notification even

[19] Article 76 AIA.

[20] The notification procedure established by Regulation (EU) 2022/2554 consists of three phases: initial notification, interim report and final report.

outside the 72-hour period if accompanied by notification of the reasons for the delay.

The ninth and tenth paragraphs of Article 73 provide two exceptions to the general duty of 73 (1) AIA.

Firstly, in the case of high-risk AI systems referred to in Annex III, which are subject to the Union legislative acts setting out reporting obligations equivalent to those set out in Article 73 AIA, notification under the AIA is not required, except in the case of incidents involving breaches of obligations under the EU law aimed at protecting fundamental rights. [21]

Annex III of the AIA includes a wide range of high-risk AI systems as long as they are part of the following areas: biometrics, critical infrastructure, education and vocational training, employment, workers' management and access to self-employment, and enjoyment of essential private services and essential public services and benefits, law enforcement, migration, asylum and border control management, administration of justice and democratic processes. In these areas, where there is a rule of EU law providing for information obligations equivalent to those of the 73, the reporting duty will be waived except where the incident concerns the fulfilment of obligations under EU law intended to protect fundamental rights. The rule includes this clause to avoid duplication of obligations as a result of overlapping rules.

A clear example is AI systems intended to be used as safety components in the management and operation of critical digital infrastructure such as road traffic and the supply of water, gas, heating and electricity. Where the incident involves critical infrastructure, there may be cases where the Artificial Intelligence Regulation [22] applies (subject in some cases to the general notification deadline and others to the special deadline discussed in section two above, which gives the provider a maximum of two days to report the incident to the Competent Authority) and simultaneously Directive (EU) 2022/2555 of the European Parliament and of the Council

[21] Article 73 (9) AIA.

[22] The definition of critical infrastructure in the AIA is set out in Article 3 (62), which refers to Article 2 (4) of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Institutions identified as critical in accordance with this Directive fall within the scope of application of the NIS2 Directive, following Article 2 (3) thereof, irrespective of their size. They are in turn classified as critical institutions based on the type of activity they perform.

of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union (NIS2 Directive) [23] applies.

Although both acts may address the same factual scenarios, the focus is entirely different: the NIS2 Directive focuses specifically on the cybersecurity of critical infrastructure and essential services in the European Union, while the AIA puts the focus on the regulation of AI and its risks and although it may address cybersecurity aspects related to high-risk AI systems, it does not replace or override the procedures set out in the NIS2 for the notification of cybersecurity incidents in critical infrastructure.

Chapter IV of the NIS2 Directive sets out the legal regime for cybersecurity by providing for notification duties in Article 23, which states that critical and important entities must notify without undue delay any significant incident [24] to their CSIRT, either directly or through the competent authority, with specific deadlines: 24 hours for early warning (when there is a suspicion) and 72 hours for initial notification (after the initial assessment has been carried out). They must also notify without delay the recipients of their services that may be affected by a significant cyber threat. They are required to provide detailed information about the incident, its impact and the measures taken, as well as to inform the recipients of the affected services by offering remedies. The CSIRT and competent authorities should share the information with other Member States and the ENISA agency.

It can be seen that the NIS2 Directive establishes a notification procedure and the responsibilities of the affected entities, constituting a more comprehensive regime, reporting obligations for users and more demanding deadlines than the AI Regulation. Ultimately, in our view, if the incident involves a critical infrastructure such as using a high-risk AI system,

---

[23] The NIS2 Directive does not contain a uniform regime for all types of entities and providers. Different legal regimes exist on the basis of a dual classification system: essential and significant entities (the latter being a residual category for all those covered by the NIS2 Directive).

[24] According to Article 23 (3) NIS2: An incident shall be considered significant if: '(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage'.

the AI Regulation will be applicable, but this does not replace the notification obligations of the NIS2.

Finally, the second exception to the general duty of notification for AI system providers is where the high-risk AI systems are security components of devices or are themselves devices, covered by Regulations (EU) 2017/745 and (EU) 2017/746, in which case serious incident reporting shall be limited to incidents involving breaches of obligations under Union law aimed at protecting fundamental rights, and shall be made to the competent national authority chosen for that purpose by the Member States in which the incident occurred. [25]

5. *References*

Castilla Barea, M., *Vigilancia postcomercialización, códigos de conducta y directrices*, in Barrio Andres, M (dir.), *El Reglamento Europeo de Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2024, 155.

[25] Article 73 (10) AIA.