ALERT MEMORANDUM

Cybersecurity Law enters into force

July 25, 2024

On July 17, 2024, Law No. 90/2024 containing provisions for strengthening national cybersecurity and addressing cybercrime (the "**Cybersecurity Law**") entered into force.

The new legislation strengthens national cybersecurity, at a time when cyber-attacks have increased significantly.[1]

The Cybersecurity Law:

(i) seeks to strengthen the resilience of (a) public administrations, (b) operators that are subject to the application of the Italian National Cybersecurity Perimeter ("**Perimeter**") legislation, (c) operators of essential services and providers of digital services, as defined in Italian Legislative Decree No. 65/2018, which implements the first EU Directive 2016/1148 on security of network and information systems ("**NIS 1 Operators**") and (d) operators providing public communications networks or publicly accessible electronic communications services ("**Telecommunication Operators**"), by establishing detailed rules on public procurement of IT goods and services that are essential for the protection of national strategic interests;

(ii) imposes new incident reporting obligations;

(iii) increases the role of the National Cybersecurity Agency (the "**NCA**");

(iv) enhances data security measures by establishing the National Cryptographic Center; and

(v) significantly focuses on the fight against cybercrime by increasing penalties for existing criminal offenses and introducing new criminal offenses in relation to individuals and entities under Italian Legislative Decree No. 231/2001 ("**Decree 231**").

The Cybersecurity Law provisions are in addition to the existing Italian cybersecurity regulatory framework, which includes, as mentioned, the Perimeter legislation (Decree Law No. 105/2019),[2] the Digital Operational Resilience Act (Regulation (EU) 2022/2554, "**DORA**"), and Italian Legislative Decree No. 65/2018, which implements the NIS 1 Directive.[3]

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

ROME

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

Andrea Mantovani
+39 06 6952 2804
amantovani@cgsh.com

Bernardo Massella Ducci Teri
+39 06 6952 2290
bmassella@cgsh.com

Federica Mammì Borruto
+39 06 6952 2826
fmammiborruto@cgsh.com

Marco Accorroni
+39 06 6952 2320
maccorroni@cgsh.com

Paola Maria Onorato
+39 06 6952 2654
ponorato@cgsh.com

MILAN

Giulia Checcacci
+39 02 7260 8224
gcheccacci@cgsh.com

Elena Galimberti
+39 02 7260 8670
egalimberti@cgsh.com

[1] According to the Report published by the Italian Association for Information Security ("**CLUSIT**") 2024, in 2023 cyber-attacks increased by 11% globally and by 65% at the Italian level.

[2] Together with the relevant implementing decrees: Italian President of the Council of Ministers' Decree ("**DPCM**") No. 131 of July 30, 2020; Italian Presidential Decree ("**DPR**") No. 54 of February 5, 2021; DPCM No. 81 of April 14, 2021; Italian Legislative Decree No. 82 of June 14, 2021; DPCM of June 15, 2021; DPCM No. 92 of May 18, 2022; and the NCA Resolution of January 3, 2023 (the "**NCA Resolution**").

[3] However, the Cybersecurity Law does not specifically refer to EU Directive 2022/2055 (the "**NIS 2 Directive**"), which Member States are required to implement by October 17, 2024.

1. SCOPE

The Cybersecurity Law imposes obligations on Public Administrations [4] and on in-house companies that provide Public Administrations with: IT services; transportation services; urban, domestic or industrial wastewater collection, disposal or treatment services; and waste management services ("**Public Operators**"). These in-house companies are included within the scope of the law as they are considered to be critical infrastructure providers, in relation to which cybersecurity vulnerabilities may impact the entire supply chain of goods and services.

In addition, the Cybersecurity Law increases some of the obligations imposed on NIS 1 Operators, Telecommunication Operators and operators included in the Perimeter.

2. INCIDENT REPORTING OBLIGATION

According to Article 1 of the Cybersecurity Law, Public Operators are required to report to the NCA all incidents impacting networks, information systems, and IT services listed in the taxonomy included in the NCA Resolution.[5]

Public Operators must submit an initial report within 24 hours of becoming aware of the incident and a complete report within 72 hours, using the channels available on the NCA website.

Public Operators may also voluntarily report incidents not included in the NCA Resolution taxonomy. These voluntary reports are processed only after mandatory ones to avoid unduly burdening the Italian Computer Security Response Team. Furthermore, submitting a voluntary report shall not impose any new obligations on the notifying party beyond what would be required if the report was not submitted.[6]

In the case of non-compliance with the reporting obligation, Article 1(5) of the Cybersecurity Law requires the NCA to issue a notice to the Public Operator, informing it that repeated non-compliance over a 5-year period will result in an administrative fine ranging from €25,000 to €125,000. Additionally, the NCA may conduct inspections within 12 months of identifying a delay or omission in compliance with the reporting obligation to verify that the Public Operator has taken steps to enhance resilience against the risk of incidents.

The incident reporting obligation takes effect immediately for central public administrations included in the Italian National Institute of Statistics ("**ISTAT**") list, as well as for regions, the autonomous provinces of Trento and Bolzano, and metropolitan cities. For all other Public Operators, this obligation will take effect 180 days after the law enters into force.

Under Article 1 of the Cybersecurity Law, the reporting obligation is extended to more entities than those included in the Perimeter. In addition, the amendment to Article 1(3-*bis*) of Italian Decree-Law No. 105/2019 (establishing the Perimeter) extends the reporting procedure and timeframes set out in the Cybersecurity Law (initial reporting within 24 hours and complete reporting within 72 hours) to incidents that affect networks, information systems, and IT services other than ICT Assets[7] of entities included in the Perimeter.

The reporting obligation under Article 1 of the Cybersecurity Law does not apply to (i) NIS 1 Operators; (ii) operators included in the Perimeter in relation to incidents affecting ICT Assets (for which the provisions of the Perimeter legislation remain applicable); (iii) State bodies in charge of public and military security; (iv) the Department of Security Information, (v) the External and Internal Information and Security Agencies.

3. ADDRESSING CYBERSECURITY VULNERABILITIES REPORTED BY THE NCA

The Cybersecurity Law outlines how to handle reports of the NCA addressed to Public Operators, entities

[4] Specifically, according to the Cybersecurity Law, the following are considered public administrations: central public administrations included in ISTAT annual list of public administrations; regions and autonomous provinces of Trento and Bolzano; metropolitan cities; municipalities with a population of more than 100,000 inhabitants and in any case, regional capitals; urban public transportation companies with a catchment area of not less than 100,000 inhabitants; suburban public transportation companies operating within metropolitan cities; and local health care companies.

[5] See https://www.gazzettaufficiale.it/eli/id/2023/01/10/23A00114/sg.

[6] See Article 18, paragraphs 3, 4 and 5 of Italian Legislative Decree No. 65/2018.

[7] Defined, in accordance with Art. 1. letter m) of DPCM 131/2020 as a "*set of networks, information systems and information services, or parts thereof, of any nature, considered unitarily for the purpose of performing essential functions of the State or for the provision of essential services.*"

included in the Perimeter, and NIS 1 and Telecommunication Operators.

In particular, the NCA may identify specific cybersecurity vulnerabilities that could affect the abovementioned recipients. These entities are required to promptly address the identified vulnerabilities within a maximum of 15 days, unless justified technical or organizational constraints prevent them from doing so immediately or necessitate postponement beyond the specified deadline.

Failure to comply with this provision will result in an administrative fine ranging from €25,000 to €125,000.

4. CONTACT PERSON AND CYBERSECURITY STRUCTURE

Public Operators must establish a cybersecurity structure and designate a cybersecurity contact person (with specific expertise). This contact person, whose name must be communicated to the NCA, will be the NCA's contact point for cybersecurity matters.

The obligations, introduced for Public Operators are similar to those provided for the entities included in the Perimeter. For instance, Public Operators are required to: (i) implement internal information security policies; (ii) maintain an information risk management plan; (iii) set out the roles and responsibilities of the parties involved; (iv) implement actions to enhance information risk management based on NCA guidelines; and (v) continuously monitor security threats and system vulnerabilities to ensure timely security updates when necessary.

5. ENHANCING DATA SECURITY MEASURES

Public Operators, as well as operators included in the Perimeter and NIS 1 Operators, must verify that computer and electronic communication programs and applications use cryptographic solutions that comply with the guidelines on encryption and password storage issued by the NCA and the Data Protection Authority. In particular, in order to prevent encrypted data from being accessible to third parties, these entities must also ensure that the applications and programs specified in the regulation are free from known vulnerabilities.

Within the framework of the national cybersecurity strategy, the NCA has an increased role in promoting cryptography. This involves the development of standards, guidelines, and recommendations to strengthen information system security. Furthermore, the NCA conducts evaluations of cryptographic system security and coordinates initiatives aimed at advocating for cryptography as a critical cybersecurity tool.

For this purpose, the Cybersecurity Law provides for the creation of a National Cryptographic Center within the NCA, which operates under the guidelines set out by the NCA's General Director.

6. PUBLIC PROCUREMENT OF ICT GOODS, SYSTEMS AND SERVICES

When procuring certain categories of ICT goods, systems and services for activities involving the protection of strategic national interests, public administrations, public service operators, publicly controlled companies,[8] and entities included in the Perimeter must ensure that the ICT goods and services acquired comply with particular criteria and technical standards, thereby safeguarding the confidentiality, integrity, and availability of processed data. These essential cybersecurity standards will be set out in a DPCM, to be adopted within 120 days of the Cybersecurity Law coming into force.

This new obligation stands alongside the existing requirement for entities included in the Perimeter to carry out an evaluation process through the Centre for National Evaluation and Certification (the "**CVCN**") to ensure the security of ICT Assets intended for deployment under the Perimeter, as set out in the DPCM dated June 15, 2021. Accordingly, entities under the Perimeter are required, in addition, to assess compliance with essential cybersecurity standards outlined in the abovementioned DPCM for ICT goods and services that are not subject to CVCN evaluation.

7. RESTRICTIONS ON PERSONNEL RECRUITMENT

The Cybersecurity Law introduces several restrictions, for private entities, to hire individuals who have held specific roles within certain central public administrations, which, if breached, will result

[8] Operators referred to in Article 2(2) of the Digital Administration Code (Italian Legislative Decree No. 82/2005).

in the contract entered into becoming null and void (Articles 12 and 13).

For instance, the Cybersecurity Law precludes, for a period of two years starting from the last training course, NCA employees who have attended, in the interest and at the expense of the NCA, specific specialized training courses, from taking positions with private entities aimed at performing cybersecurity-related tasks.

8. AMENDMENTS TO THE DORA REGULATION SCOPE

Lastly, the Cybersecurity Law amends the law implementing the DORA regulation to include, in addition to "financial entities", financial intermediaries[9] and Poste Italiane S.p.A in relation to its Bancoposta business.

The objective of this amendment is to ensure a high level of digital operational resilience and to maintain stability across the financial sector. Consequently, in the exercise of the delegated power, the Government will make the appropriate adjustments and additions to the regulations governing these entities to align their operational resilience measures with those outlined in the DORA Regulation. These changes will apply to the activities undertaken by each entity concerned. Additionally, the Bank of Italy will assume supervisory, investigative, and sanctioning responsibilities over these entities.

9. MAIN AMENDMENTS TO THE REGULATION ON CYBERCRIME

The Cybersecurity Law strengthens the fight against cybercrime by introducing significant amendments to both the Italian Criminal Code (the "**ICC**") and the Italian Code of Criminal Procedure (the "**ICCP**").

In particular, the Cybersecurity Law:

- Increases criminal penalties for a range of cybercrimes, including the crime of unauthorized access to computer systems and the crime of destruction of computer data, information, and programs;

- Introduces new aggravating circumstances. It extends the aggravating circumstance which applies when the crime is committed "*by a public official or a person in charge of a public service, through abuse of power or in violation of the duties of his or her position or service, by a person who, also abusively, exercises the profession of private investigator, or by abuse of the position of computer system operator*", to apply to all cybercrimes covered by the Cybersecurity Law. It introduces a new aggravating circumstance for the crime of fraud in cases where the act is committed remotely by means of computer or telematic tools capable of impeding one's own or another's identification.[10] It also increases the penalties provided for the existing aggravating circumstances;

- Introduces two new mitigating circumstances (Articles 623-*quater* and 639-*ter* ICC), applicable to specific cybercrimes, [11] which can reduce penalties by (i) up to one-third if the crime can be considered to be "*minor*" because of the manner in which it was committed, or if the damage or risk is particularly insignificant; (ii) from one-half to two-thirds if the offender takes steps to prevent further consequences of the crime. This includes actively assisting the authorities in gathering evidence or recovering the proceeds of the crime or the instruments used to commit the crime;

- Repeals Article 615-*quinquies* ICC, which punishes the unlawful possession, distribution and installation of instruments, devices or programs designed to damage or interrupt a computer or telematic system, and replaces it with

[9] Listed in the register provided for in Article 106 of the Consolidated Law on Banking and Credit, referred to in Italian Legislative Decree No. 385/1993.

[10] New paragraph 2-*ter* of Article 640 ICC.

[11] In particular, Article 623-*quater* ICC applies to the criminal offenses set out in Articles 615-*ter* (Unauthorized access to a computer or telematic system), 615-*quater* (Possession, distribution and unauthorized installation of tools, codes and other means of access to computer or telematic systems), 617-*quater* (Unlawful interception, obstruction, or disruption of computer or telematic communications), 617-*quinquies* (Possession, distribution and unauthorized installation of tools and other means to intercept, obstruct or interrupt computer or telematic communications) and 617-*sexies* ICC (Falsifying, altering or suppressing the content of computer or telematic communications). Article 639-*ter* ICC instead applies to the criminal offenses set out in Articles 629(3) (new crime of cyber-extortion), 635-*ter* (Damage to information, data and computer programs of a public nature or interest), 635-*quarter*.1 (Unauthorized possession, distribution, or installation of tools, devices, or programs designed to damage or interfere with a computer or telematic system) and 635-*quinquies* ICC (Damage to public utility computer or telematic systems).

the new criminal offense outlined in Article 635-*quater*.1 ICC; [12]

- Introduces the new crime of cyber-extortion (Article 629(3) ICC), which punishes by imprisonment of 6 to 12 years and a fine of € 5,000 to € 10,000 (penalties that may be increased if certain aggravating circumstances are met) [13] anyone who, by committing or threatening to commit specific cybercrimes, [14] forces another person to do or refrain from doing something in order to obtain an unjust benefit for himself or herself or for others to the detriment of others. For example, the new crime could apply in cases where a person, having hacked into a computer system and manipulated or damaged information, data or programs, demands a ransom for the restoration of the computer system and its data.

In addition, the Cybersecurity Law provides for: (i) the allocation of the preliminary investigation of cybercrimes to the district prosecutor's office; (ii) the application of a "*simplified*" system for granting an extension of the preliminary investigation period for cybercrimes; [15] and (iii) the extension of the maximum period for preliminary investigation to two years.

10. AMENDMENTS TO DECREE 231 AND NEXT STEPS FOR COMPANIES

The Cybersecurity Law introduces significant amendments to Decree 231. In particular, the Cybersecurity Law:

- Increases the penalties for cybercrimes established by Article 24-*bis* of Decree 231, providing for (i) a maximum fine of € 1,084,300 for the offenses referred to in Article 24-*bis*(1) of Decree 231, [16] and (ii) a maximum fine of € 619,600 for the offenses referred to in Article 24-*bis*(2) [17] of Decree 231; [18]

- Expands the list of crimes that may trigger liability for companies and other legal entities under Decree 231, by including the new crime of cyber-extortion (new Article 24-*bis*(1-*bis*) of Decree 231) which is subject to the following penalties (i) a maximum fine of € 1,239,200, and (ii) disqualification penalties set out in Article 9(2) of Decree 231 (*i.e.*, disqualification from conducting business; suspension or revocation of authorizations, licenses or concessions instrumental to the commission of the crime; prohibition from entering into contracts with the public administration; exclusion from grants, loans, contributions and subsidies with the possible revocation of those already granted; and ban on advertising goods and services) for a period of at least two years.

In light of these developments, companies should consider reviewing and updating their policies and procedures to ensure that they are adequate to prevent new offenses that may trigger liability under Decree 231. In particular, companies should consider implementing new and more specific control measures, in addition to those already in place to prevent the commission of cybercrimes (which may already constitute a safeguard, even with respect to the newly introduced crime of cyber-extortion). Measures may include ensuring the proper use of IT tools, maintaining security standards for user identity, data integrity and confidentiality, monitoring employee network usage, and providing targeted information and training to company personnel.

11. CONCLUSION

The new Cybersecurity Law, while fitting into a complex regulatory framework that will need further changes, including in the short term (consider, in this

[12] The new provision addresses the same conduct for which penalties were provided for under former Article 615-*quinquies* ICC and provides for the same penalties, with the addition of the aggravating circumstances set out in Article 615-*ter*(2.1) and Article 615-*ter*(3) ICC.

[13] In particular, a penalty of imprisonment of 8 to 22 years and a fine of € 6,000 to € 18,000 applies if the aggravating circumstances referred to in the paragraph 3 of Article 628 ICC (i.e., the aggravating circumstances provided for the crime of robbery) are met, or where the crime is committed against a person incapacitated by age or infirmity.

[14] That is, those set out in Articles 615-*ter*, 617-*quater*, 617-*sexies*, and 635-*bis* (Damage to computer information, data and programs), 635-*quater* (Damage to computer or telematic systems) and 635-*quinquies* ICC.

[15] In particular, the "*simplified*" regime is provided for under Article 406(5-*bis*) ICCP, which provides that the judge shall issue an order within ten days from the submission of the request for extension of the preliminary investigation period by the public prosecutor. This provision, which is reserved for particularly serious crimes, is intended to allow a more timely and effective investigation of the commission of the crime.

[16] That is, the crimes under Articles 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* and 635-*quinquies* ICC.

[17] That is, the crimes under Articles 615-*quater* and 635-*quater*(1) ICC.

[18] The disqualification penalties provided for these cybercrimes remain unchanged.

regard, that as early as October 2024 the NIS 2 Directive will have to be implemented) nevertheless represents a concrete response to the sudden and substantial increase in cyber threats. In particular, the expansion of incident reporting requirements to include new stakeholders and the introduction of stricter reporting deadlines for incidents not affecting ICT Assets aim to enhance national cyber resilience and security. This approach ensures that critical infrastructure providers have better control over cybersecurity incidents.

The increased penalties for cybercrimes, the introduction of new criminal offenses, and the developments regarding corporate liability under Decree 231 are also consistent with the above objectives. These measures are intended to tackle the increasing threat of cybercrime, although their effectiveness in practice remains to be seen.

…

CLEARY GOTTLIEB