

Information and technology law course

LECTURE 6 – 10 OCTOBER 2023

FEDERICA CASAROSA – 2024/2025

From NIS Directive to Italian implementation

Implementation: translate and pull it into a law, but keep in mind of possible convergences with other laws to keep in mind what the existing basis is.
We need to check how impl. has been translated into the italiano context.

Existing legal framework - 1

Legislative Decree No. 82 of 2005 (Digital Administration Code)

- Article 51 : initial intervention on data security ①

Codice dell'amministr. digitale: collection of several elements that were in different laws.

Law No. 155/2005 on urgent measures to combat international terrorism

- Article 7a on cyber security: cyber protection services of critical digital infrastructures of national interest were allocated to the Ministry of the Interior

③

④

① Related to the fact that data used in public admin. has to be secured.

② Another law. Security perceived as something to be tackled.

③ We still didn't have the Critical Infra. directive but there was an idea of critical infrastr. essential for the work of society, identified as mkt. interests.

The ④ was assigned to determine the rules.

Existing legal framework - 2

Law No. 134/2012 on Italian Digital Agenda ①

- Creation of Agenzia per l'Italia Digitale coordinating “actions in the field of innovation to promote ICT technologies to support public administrations, guaranteeing the realisation of the objectives of the Italian Digital Agenda, in coherence with the European Digital Agenda”

Prime Minister's Decree of January 24, 2013, on cyber protection and national cybersecurity

- Coordination of cybersecurity-related activities involving public administrations and the intelligence community.

National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace and Cybersecurity

- Internal organisation to enable timely and coordinated responses to cyber threats targeting national assets

- ① There was in 2011 a surge in terrorism. The agency created is an authority at national level to coordinate innovations. Activities to support public admin. This in coherence with the EU digital agenda.
- ② Still regarding public admin, so no private companies.
Trying to figure out a system to deal with those kind of activities. There was a project on security - national defense - critical infrastructure.

In ① more about digital policies, but the others regarding security only public administration.

Legislative decree vs law: Decree law: document promulgated quickly by the parliament that requires approval to become law.
Law ≈ legislative decree.

Set of interventions

To implement NIS not a single law was sufficient.

Legislative Decree No. 65 of May 18, 2018 implementing NIS Directive

National Cybersecurity Perimeter with the Decree-Law of September 21, 2019 (Perimeter Decree).

D.P.C.M. No. 131 of July 30, 2020

D.P.C.M., No. 81 of April 14, 2021

Presidential Decree No. 54 of February 5, 2021

DL No. 82/2021

↳ documents that are the same binding authority of legislative decree
but more easily modifiable.

Decreto Legislativo 65/2018

Decreto **Legislativo 18 maggio 2018**, n. 65, attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

- Article 1
- **Measures aimed at achieving a high level of network and information security at the national level, thereby contributing to increasing the common level of security within the European Union.**

Same structure of the NIS. In this case we need to turn general measures into a better def. of who does what.

Decreto Legislativo 65/2018

Articles 12 and 14 Entities obliged to report incidents.

→ obligation set + specification.

- OES and DSP are subject to an obligation to report incidents or attacks to the CSIRT.
- NB For other entities, incident reporting is optional

SANCTIONS

Article 21 addresses the case of lack of compliance: if cybersecurity obligations are not fulfilled by private entities, a set of administrative sanctions can be imposed by competent NIS authorities.

- OES does not take appropriate and proportionate technical and organisational measures for network and information system security risk management or take appropriate measures to prevent and minimise the impact of incidents
 - administrative fine ranging from EUR 12,000 to EUR 120,000
- DSP does not take appropriate and proportionate technical and organisational measures for network and information system security risk management or take appropriate measures to prevent and minimise the impact of incidents
 - administrative fine ranging from EUR 9,000 to EUR 90,000
- OES or DSP fails to notify the Italian CSIRT of incidents having a significant impact on the continuity of the essential services provided
 - administrative fine ranging from EUR 25,000 to EUR 125,000
- OES dependent on a third party DSP for the provision of a service that is indispensable for the maintenance of fundamental economic and social activities fails to notify
 - administrative sanction ranging from 12,000 euro to 120,000 euro.

- ① Implement the measures, first of all (will have to say which ones) and take measures to prevent and minimise the impact.
- ② Some applies for DSP, but those actions are perceived as a bit less important.
- ③ If you don't modify, sending is the same.
- ④ According to IT and NIS, OES is no change of the modif.

↑ first step that provokes the document

Decr. legge 105/2019 (Legge 133/2019)

National cybersecurity perimeter (Perimetro di sicurezza nazionale cibernetica - PSNC) to complement European regulations by involving all public or private operators

- even outside the scope of NIS Directive but that are essential for Italian national security.

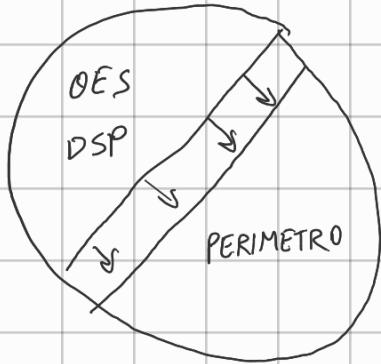
(1) Objective : high level of security for networks, information systems, and IT services of public administrations, as well as national public and private entities

(2) Measures aimed at ensuring the necessary security standards to minimize risks

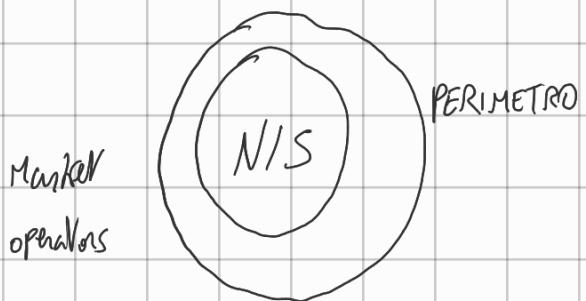
- criteria for identifying the entities included in this perimeter were established by the D.P.C.M. 131/2020 which distinguishes between essential functions and services.

2 types of actors: going from legislative decree 65/2018 that implemented NIS, the legislative decree 2019 that became law 133/2019 to go further.

IT legislators identified a problem: I have a set of companies that are OES and DSP. But they are not all the critical infrastructure that are relevant to me.



In 2019 the decree legal was outside the scope of the NIS. They were using the measures of the NIS to expand them to other critical companies. The obligations of the NIS and of the Perimeters are exactly the same.



We extend the scope to companies essential for national security. (1)

Legge sul perimetro was just extending. (2)

DPCM
131/2020

Essential functions :

- ensuring the continuity of government action and constitutional bodies, *(coorte costituzionale)*
- internal and external security,
- defense of the State, *Military*
- international relations,
- public safety and order,
- administration of justice, *coorte dei conti, cassazione*
- the functioning of the economic and financial systems and transportation (Art. 2).

Those fall into perimeter

Essential services (tasks performed for the maintenance of fundamental civil, social, or economic activities in the interests of the State):

- activities instrumental to the exercise of essential State functions *law enforcement*
- activities necessary for the exercise and enjoyment of fundamental rights *(freedom of speech)*
- activities necessary for the continuity of supplies and the efficiency of infrastructure and logistics
- research activities and activities related to productive sectors in high technology and any other sector, where they have economic and social relevance, including the guarantee of national strategic autonomy, competitiveness, and development of the national economic system.

The Cybersecurity perimeter applies only to networks, information systems, and IT services whose malfunction, interruption, or improper use could pose a threat to national security

Can decide if an org. with economic relevance

Whatever company can fall into this.

In 2020 we thought "it's not enough what the NIS was doing".

DPCM 81/2021 – 1

Obligations related to

- prevention activities and
- incident notification and response

Procedure :

- Entities included in the Perimeter receive notification of their inclusion in the list
- In six months the entities have to prepare lists of networks, information systems, and IT services
 - This list will be subject to at least annual updates to align with the actual state of the entity's infrastructure
- Risk analysis on their ICT assets and an analysis of the effects of an interruption and/or compromise of their operations, as well as assessments of mitigation measures.
- Adopt measure to ensure levels of protection based on internationally and EU-defined standards
 - Standard based on NIST framework for cybersecurity

↓
Standard created in the US for cybersc.

↑ National authority for cybersecurity (ACN) is in charge.

↓ No standards for now

(1) Evaluate what are your elements to be secured.

*

Choice was to use the NIST because it represented state of the art measures. There are countries that use ISO and others NIST. The main one is the one that dictate the standard. But, NIST framework doesn't take into account personal data. So we added something more regarding personal data protection.

DPCM 81/2021 – 2

We have controls and highly controls: 6 vs 12 hours to notify for the incident.

Incident notification

- Two classes of incidents : classification based on severity.
- Different degrees of severity determine different notification deadlines

These notifications are directed to the Italian CSIRT. Violation of these provisions can lead to the imposition of very high sanctions.

Presidential decree 54/2021 – 1

Entities should communicate to the national evaluation and certification center (Centro di Valutazione e Certificazione Nazionale – CVCN) any outsourced supply of products and services

- CVCN assess the security of ICT goods, systems, and services intended for use within the perimeter and falling within the categories specified by the Decree of June 15, 2021
- Decreto del Presidente del Consiglio dei Ministri -D.P.C.M.- 15 giugno 2021. Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105

Who is monitoring? There's an entity CVCN, inside the national authority. It has the task of measures to check if you adopted the measures. The verification applies for NIS and Penetration and this applies to the ICT. What happens if I want to outsource a certain service? You make a "bestow or gain" in which companies offer their service, I have to check the offers with the CVCN to see if you can make a contract with an organization. You can't even justify the fact that you reject their offer because you can't say that for security reasons someone else is better. You create a system in which the control is good but creates a huge problem because you have to comply the rule of accepting the best offer, otherwise it is discrimination. Balance security and the freedom of business.

Presidential decree 54/2021 – 2

Entities should notify the CVCN of their intention to acquire ICT goods, systems, and services to be used in strategic areas

- notification includes a description of the subject of the supply, its use and category, information and services treated in the supply, and an analysis of the associated risk related to the supply, including the scope of use, the description of the operating environment, components interacted with, and security measures.

Process:

- CVCN provides instructions and conditions to be followed within 60 days
- Hardware and software tests to be completed within sixty days at the CVCN itself or at facilities accredited by it
- CVCN will communicate the outcome and any usage prescriptions aimed at ensuring security.

OK, best offer is the good one but you have to have tests, and the businesses shouldn't know why. "You have to go there to have your product tested". Facilities accredited by ACN will provide. And the facilities shouldn't be public!

Decr. Legge 82/2021

National governance of the cybersecurity system

Italian Cybersecurity Authority - Agenzia per la Cybersicurezza Nazionale (ACN)

Organization similar to other administrative agency

- Legal personality and regulatory, administrative, patrimonial, organizational, accounting, and financial autonomy
- NB: technical and specialized functions with a political direction and control BUT with a greater degree of autonomy to ensure a certain degree of independence from political power due to potential conflicts with the protection of fundamental rights
- The Agency is subject to the directives of the Presidente del Consiglio and the oversight of COPASIR (Comitato parlamentare per la sicurezza della Repubblica)

Administrative agency: authorities that have legal personality, they have autonomy regarding national regulations...

All of them have to report their activity to the parliament, but we have a bit more autonomy to prevent control from policies and political control - Only control: they have to report to the President.

Decr. Legge 82/2021

National governance of the cybersecurity system

- Presidente del Consiglio dei Ministri
 - responsible for the overall direction of cybersecurity policies, including the adoption of the national strategy and the leadership of the new Italian cybersecurity agency
- Italian Cybersecurity Authority - Agenzia per la Cybersicurezza Nazionale (ACN) – technical function
- Interministerial Committee for Cybersecurity (Comitato Interministeriale per la Cybersicurezza - CIC) – political function
 - organization with advisory, proposal, and oversight functions regarding cybersecurity policies

Because NR's controlling



(linee guida politiche e coord. tra organi)

Technical side

Italian Cybersecurity Authority – 1

Agenzia per la Cybersicurezza Nazionale (ACN)

Organization similar to other administrative agency

- Legal personality and regulatory, administrative, patrimonial, organizational, accounting, and financial autonomy
- NB: technical and specialized functions with a political direction and control BUT with a greater degree of autonomy to ensure a certain degree of independence from political power due to potential conflicts with the protection of fundamental rights
- The Agency is subject to the directives of the Presidente del Consiglio and the oversight of COPASIR (Comitato parlamentare per la sicurezza della Repubblica)

Objectives

- technical functions aimed at safeguarding national interests in the field of cybersecurity and promoting common actions to ensure cybersecurity
- developing national capabilities for prevention, monitoring, detection, analysis, and response to prevent and manage cybersecurity incidents and cyberattacks.
- prevention and prosecution of cybercrimes and national security and defense still remain allocated to Ministro dell'Interno and the Ministro della Difesa.

everything done by them except cybercrime and cyber defense.

1. Ensure private-public coop.
2. Develop abilities to counter incidents and attacks.
3. Support research
4. Check
5. Cooperate EU level
6. Improve security of pub. info infra.

Italian Cybersecurity Authority – 2

Tasks

- preparation of the national cybersecurity strategy and in coordinating activities among the entities (public and private) involved.
- Develop preventive and reactive capabilities to counter incidents and cyberattacks.
- Develop national digital industry and improving the security of public information infrastructures, also through product, process, and ICT system certification activities.
 - Issue non-binding opinions on regulatory and legislative strategies in the field, with the aim of achieving the definition and maintenance of an updated and coherent national legal framework in the domain of cybersecurity, also taking into account international trends and developments.
- Coordinate cooperation at the European and international levels in the field of cybersecurity.
- Support research, innovation, and the development of scientific and professional skills in the sector.
- ③ ◦ Conduct inspection, verification, and enforcement activities regarding violations by private entities falling within the national cybersecurity perimeter (PSNC), and if necessary, it can issue specific prescriptions and impose administrative sanctions as provided by the decree establishing the PSNC

Role Everything to the ACN

- National supervisory authority
- CSIRT-Italy Tasks of a CSIRT at multi level and represents IT at national level
- Single point of contact for network and information system security
- National certification authority We'll see
- CVCN works like the CVCN.

provides all

(2) Working to collaborate with companies to prevent the attack and help them.

(3) They knock on your door.

But there are other actions from A

Italian CSIRT

1. Monitor incidents 2. Analyze risks and make 3. Awareness 4. Raise awareness, with alerts, announcements; networks

Tasks:

- monitoring incidents at the national level;
- issuing pre-alarms, alerts, announcements, and information dissemination to relevant parties regarding risks and incidents; *Not just some theory they do on request,*
 - e.g. sharing data related to new vulnerabilities through publication on its website
- intervening in the event of an incident;
- dynamically analyzing risks and incidents;
- carrying out situational awareness activities
- being part of the so-called network of CSIRTS that interacts with ENISA

Implementation of NIS 2 Directive

Molte
DECRETO LEGISLATIVO 4 settembre 2024, n. 138 *New legislative decree*

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

Identification of Essential and important entities

- ACN will draw up the list of the companies and PAs involved by April 2025
- All entities will have to register from the date of publication on a special platform at ACN (*Special platform*)

Security obligations *→ work the DPCM for the level of details*

- Not mentioned in the text but to be defined by the ACN on the basis of
 - the degree of exposure to risk
 - the size of the entity;
 - the probability of incidents occurring; and
 - the severity (including the economic and social impact).

It is possible that we will have the modification of all of the laws defined for NIS.

Now the threshold for EE/IE has changed.

More than 150 employees is medium size enterprise. The newcomers are the problem: They are big enough to be included that need to invest more into the adoption of measures.

Id. will be up to the ACN.

Implementation of NIS 2 Directive

Sanctions

- The sanctioning treatment is differentiated according to the type of violation
 - non-compliance with the obligations imposed on the management bodies; failure to implement technical, organisational and operational measures; failure to notify.
 - EEs : up to 10 million or up to 2% of the total annual worldwide turnover for the subject's previous financial year
 - IE: up to 7 million or up to 1.4% of the total worldwide turnover
 - the failure to register, communicate or update information on the ACN platform; failure to comply with the procedures established by ACN for the registration, communication or updating of data; failure to communicate or update the list of activities and services for the purposes of their categorisation; failure to implement obligations relating to certification schemes; failure to cooperate with the ACN in carrying out its tasks and exercising its powers; failure to cooperate with the CSIRT Italia.
 - EE: up to 0.1 per cent of the annual turnover
 - IE: up to 0.07 per cent of the annual worldwide turnover
 - In the event of repeated violations, sanctions may be increased up to threefold
 - Accessory sanctions
 - In the event of a warning from the ACN requiring the implementation of certain measures being ignored, it is possible to temporarily suspend a certificate or authorisation relating to the services provided by the subject.

↳ additional activities. (cybersecurity certifications)