Sovranità Digitale e Cybersecurity

Cosa dicono le normative europee e perché

Avv. Valerio Edoardo Vertua

CEFRIEL - Milano - 02.12.2025

$whoami

Avvocato Cassazionista - Partner di 42 LawFirm s.r.l. Società tra Avvocati
Settori di attività prevalente:
diritto tributario - societario, diritto dell'informatica e delle nuove tecnologie
Ordine degli Avvocati di Milano

Perfezionato in Diritto Societario
Perfezionato in Computer Forensics ed Investigazioni Digitali
Perfezionato in Data Protection e Data Governance
Perfezionato in Strategie Avanzate di Applicazione del GDPR
Perfezionato in Legal Tech, Coding for Lawyers, AI e Blockchain Legal Issues
Università degli Studi di Milano

Collaboratore della Cattedra di Informatica Giuridica e Informatica Giuridica Avanzata
Facoltà di Giurisprudenza - Università degli Studi di Milano

Associazioni:

Il framework normativo UE

Cinque pilastri per la sicurezza digitale europea

DIRETTIVA

NIS2

2022/2555

Sicurezza reti e sistemi per operatori essenziali

- 18 settori coinvolti
- Obblighi governance
- Notifica 24-72h
- Sanzioni fino €10M

REGOLAMENTO

CRA

2024/2847

Cyber Resilience: sicurezza prodotti digitali

- Security by design
- Marcatura CE cyber
- Aggiornamenti 10 anni
- In vigore dic. 2027

REGOLAMENTO

DORA

2022/2554

Resilienza operativa settore finanziario

- Banche, assicurazioni
- Test di resilienza
- Gestione fornitori ICT
- Applicabile gen. 2025

REGOLAMENTO

Cyber Solidarity

2025/38

Cooperazione UE emergenze cyber

- Sistema allerta UE
- Riserva emergenza
- Risposta coordinata
- In vigore feb. 2025

REGOLAMENTO

AI Act

2024/1689

Regolamentazione sistemi di intelligenza artificiale

- Classi di rischio AI
- Obblighi trasparenza
- Sanzioni fino 35M€
- In vigore ago. 2025

La risposta dell'Italia

Dal Perimetro nazionale al recepimento direttive UE

2019

Perimetro Sicurezza Nazionale Cibernetica

D.L. 105/2019 - Protezione asset strategici - Notifica 1-6h

2021

Agenzia per la Cybersicurezza Nazionale

D.L. 82/2021 - Autorità nazionale unica - Coordinamento

2024

Recepimento NIS2

D.lgs. 138/2024 - 80+ tipologie soggetti - Sanzioni €10M o 2%

2024

Legge 90/2024 - Rafforzamento Cybersecurity

Referente cybersicurezza - Crittografia - Reati informatici

2025

Legge 132/2025

Disposizioni in materia di intelligenza artificiale

CHI È COINVOLTO

PA Centrali e Locali

Ministeri, Regioni, Comuni, ASL

Settori Critici

Energia, trasporti, sanità, finanza

Supply Chain

Fornitori ICT di soggetti essenziali

ACN = punto di contatto unico per NIS, DORA e Perimetro, AI

Perché l'Europa ha agito

Un cambio di paradigma: dalla reazione alla prevenzione

IL PROBLEMA

Dipendenza tecnologica da Paesi extra-UE per hardware, software e servizi critici

I RISCHI

Attacchi cyber in crescita: +65% nel 2024 su infrastrutture critiche UE

LA RISPOSTA

Autonomia strategica + standard comuni = resilienza europea

I DRIVER NORMATIVI

1. Geopolitica: tensioni e crisi di fiducia con fornitori terzi
2. Frammentazione: 27 approcci diversi = vulnerabilità
3. Competitività: standard come vantaggio globale
4. Valori: tutela dei diritti fondamentali nel digitale

Fonte: ENISA Threat Landscape 2024

Europa - Italia

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Luxembourg

Cloud Sovereignty Framework

Version 1.2.1 – Oct. 2025

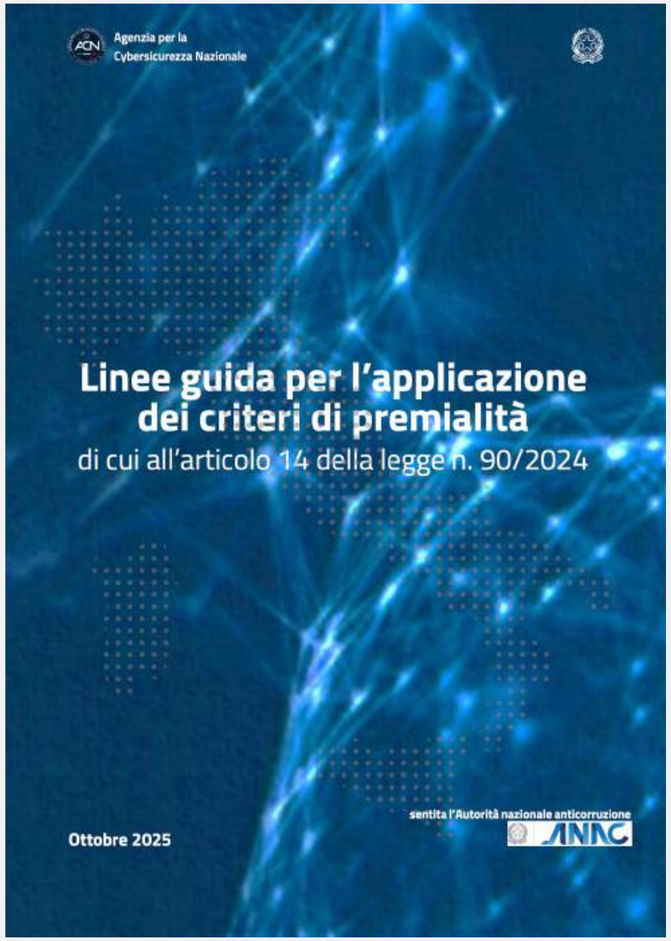
CONTENTS

$$Sovereignty\ Score = \sum_{n=1}^{n=8} \frac{Score(SOV_n)}{Max.Score(SOV_n)} \times Weight(SOV_n)\ \%$$

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË – Tel. +32 22991111

Commission européenne, 2920 Luxembourg, LUXEMBOURG – Tel. +352 4301

Tel. direct line +352 4301-32243



Cosa significa concretamente

Tre concetti chiave da portare a casa

1. **Non solo compliance**
   La cybersecurity diventa requisito di governance: responsabilità degli organi apicali

2. **Approccio risk-based**
   Misure proporzionate al rischio, non one-size-fits-all: mappatura e gestione continua

3. **Supply chain = perimetro esteso**
   Anche i fornitori sono parte dell'equazione: clausole, audit, gestione terze parti

LA SFIDA APERTA

Sovranità non significa isolamento. Bilanciare la riduzione delle dipendenze con l'apertura al mercato globale.

IN SINTESI

L'Europa ha costruito uno dei framework normativi cyber più avanzati al mondo. Ora tocca alle organizzazioni tradurlo in pratica.

v.vertua@42lf.it

Grazie per l’attenzione