

Casarosa

Definizione di legge sulla cybersecurity

Gli attacchi informatici sono cresciuti rapidamente in termini di scala, portata e sofisticazione. Quattro categorie di minacce diverse e sovrapposte:

- Guerra informatica
- Spionaggio informatico
- Terrorismo e vandalismo informatico
- Criminalità informatica

Sicurezza informatica

La cybersecurity è un termine che copre un'ampia gamma di attività volte a prevenire e mitigare le minacce informatiche:

- Sicurezza delle reti e delle informazioni
- Lotta al crimine informatico e difesa informatica

Legge sulla cybersecurity

Per definire la legge sulla cybersecurity dobbiamo rispondere a cinque domande fondamentali:

1. Cosa stiamo mettendo in sicurezza?
2. Dove e chi stiamo mettendo in sicurezza?
3. Come ci assicuriamo?
4. Quando ci mettiamo in sicurezza?
5. Perché stiamo mettendo in sicurezza?

Rispondiamo a queste domande:

1. Cosa stiamo mettendo in sicurezza?
 - a. promuovere la **riservatezza**, l'**integrità** e la **disponibilità** delle informazioni, dei sistemi e delle reti
 - b. La cybersecurity non si limita solo alla sicurezza dei dati
 - c. La cybersecurity non si concentra solo sulla protezione dei dati, ma anche dei sistemi e delle reti del settore pubblico e privato.
 - i. **Riservatezza**: prevenzione della divulgazione non autorizzata di informazioni.
 - ii. **Integrità**: garantisce che il messaggio inviato sia identico a quello ricevuto e che il messaggio non sia stato alterato durante il transito.
 - iii. **Disponibilità**: garanzia che le informazioni siano disponibili per l'utente in modo tempestivo e ininterrotto quando sono necessarie, indipendentemente dalla posizione dell'utente.
2. Dove e chi stiamo assicurando?
 - a. La legge dovrebbe concentrarsi solo sul rafforzamento della sicurezza dei sistemi governativi militari e civili?
 - b. Le leggi dovrebbero essere applicate anche alla sicurezza informatica del settore privato?
 - i. La progettazione di Internet prevede un'infrastruttura diversa per il settore pubblico e privato? NO
 - c. Qualsiasi regime normativo efficace in materia di cybersecurity cercherà di proteggere sia il settore pubblico che quello privato.
3. Come ci assicuriamo?
 - a. Hard law o soft law?
 - i. Le leggi coercitive scoraggiano l'inadeguatezza della cybersecurity, mentre quelle cooperative incentivano le aziende e le agenzie governative a investire nella cybersecurity.
4. Quando ci mettiamo in sicurezza?
 - a. La legge deve concentrarsi su eventi che si sono già verificati o deve cercare di costruire la resilienza per prevenire attacchi futuri?
 - b. È necessario un approccio lungimirante

5. Perché stiamo mettendo in sicurezza?

a. Tre tipi distinti di danni che la legge sulla cybersecurity dovrebbe cercare di evitare (o almeno di attenuare):

- i. (1) danni alle persone
- ii. (2) danni agli interessi commerciali
- iii. (3) danni alla sicurezza nazionale

Flessibilità e adattabilità delle misure

Importanza del fattore umano

Aggiornamento rispetto all'evoluzione dei rischi

Cooperazione e condivisione delle informazioni

Competenza dell'UE in materia di cibersicurezza

Competenza dell'UE

In base al **principio di attribuzione**, l'Unione agisce solo nei limiti delle competenze che le sono state conferite dagli Stati membri trattati e per raggiungere gli obiettivi in essi indicati.

Art. 4 TFUE (Trattato sul funzionamento dell'Unione europea)

1. Ai sensi dell'articolo 5, le competenze non attribuite all'Unione dai trattati restano agli Stati membri.
2. L'Unione rispetta l'uguaglianza degli Stati membri di fronte ai trattati nonché la loro identità nazionale, insita nei loro strutture fondamentali, politiche e costituzionali, comprese le autonomie regionali e locali. Rispetterà le loro strutture essenziali funzioni statali, tra cui garantire l'integrità territoriale dello Stato, mantenere l'ordine pubblico e salvaguardare la sicurezza nazionale. In particolare, la sicurezza nazionale rimane di esclusiva competenza di ciascuno Stato membro.

Qual è la base giuridica della legislazione dell'UE sulla cybersecurity?

- Articolo 114 TFUE - Mercato interno
 - Questo articolo consente all'UE di adottare misure per l'armonizzazione delle leggi negli Stati membri al fine di garantire il corretto funzionamento del mercato interno. Fornisce una base giuridica per l'allineamento normativo tra i Paesi al fine di eliminare gli ostacoli al commercio e alla concorrenza all'interno dell'UE.
- Articolo 62 e 53, paragrafo 1, del TFUE - diritto di stabilimento e libertà di prestazione di servizi
 - L'articolo 62 riguarda le disposizioni necessarie per garantire la libertà di stabilimento e la libera prestazione di servizi all'interno dell'UE. Fa riferimento agli articoli 51-54, che prevedono limitazioni e regole specifiche per la libertà di stabilimento.
 - L'articolo 53, paragrafo 1, consente al Parlamento europeo e al Consiglio di emanare direttive per il riconoscimento reciproco dei diplomi, certificati e altre qualifiche. Agevola la libertà di stabilimento, facilitando l'esercizio della professione in diversi Stati membri.
- Articolo 127, paragrafo 2, 132, paragrafo 1, del TFUE - funzionamento regolare dei sistemi di pagamento
 - L'articolo 127, paragrafo 2, delinea l'obiettivo primario del Sistema europeo di banche centrali (SEBC) di mantenere la stabilità dei prezzi. Nel perseguire questo obiettivo, il SEBC è tenuto a sostenere le politiche economiche generali dell'UE, contribuendo agli obiettivi dell'Unione.
 - L'articolo 132, paragrafo 1, conferisce alla Banca centrale europea (BCE) l'autorità di emanare regolamenti, prendere decisioni, formulare raccomandazioni e fornire consulenza, se necessario, per adempiere ai propri compiti nell'ambito del SEBC.
- Articolo 83, paragrafo 1, del TFUE - spazio di libertà, sicurezza e giustizia
 - L'articolo 83, paragrafo 1, fornisce una base per stabilire norme minime per i reati e le sanzioni nelle aree di criminalità particolarmente grave con una dimensione transfrontaliera. Ciò include il terrorismo, il traffico di esseri umani, il riciclaggio di denaro e la criminalità informatica.
- E per quanto riguarda il coordinamento a livello dell'UE - articolo 74 del TFUE
 - L'articolo 74 consente al Consiglio di adottare misure per assicurare la cooperazione tra le autorità amministrative degli Stati membri. Tale cooperazione è essenziale per il funzionamento efficace delle politiche e dei programmi attuati nell'ambito del TFUE, in particolare nei settori che richiedono un'applicazione transfrontaliera.

Nei settori che non rientrano nella competenza esclusiva dell'Unione, deve essere rispettato il principio di sussidiarietà Art. 5 TFUE

3. In base al principio di sussidiarietà, nei settori che non rientrano nella sua competenza esclusiva, l'Unione interviene **solo se e nella misura in cui gli obiettivi dell'azione proposta non possono essere conseguiti in misura sufficiente dagli Stati membri**, né a livello centrale né a regionale e locale, ma possono, a motivo della portata degli effetti dell'azione proposta, essere conseguiti meglio a livello di Unione.

- Le istituzioni dell'Unione applicano il principio di sussidiarietà come stabilito nel Protocollo sull'applicazione dei principi di sussidiarietà e proporzionalità. I Parlamenti nazionali garantiscono il rispetto del principio di sussidiarietà secondo la procedura stabilita in tale Protocollo.
- 4. In base al principio di proporzionalità, **il contenuto e la forma dell'azione dell'Unione non vanno al di là di quanto necessario per il raggiungimento degli obiettivi dei trattati.**
- Le istituzioni dell'Unione applicano il principio di proporzionalità come stabilito nel Protocollo sull'applicazione dei principi di sussidiarietà e proporzionalità.

Interventi dell'UE in materia di sicurezza informatica

- 1992, Decisione del Consiglio 92/242/CEE in materia di sicurezza dei sistemi informativi.
- 1995, Raccomandazione del Consiglio 1995/144/CE sui criteri comuni di sicurezza delle tecnologie dell'informazione
- 2001, Comunicazione sulla sicurezza delle reti e dell'informazione
 - le misure politiche possono rafforzare il processo di mercato e allo stesso tempo migliorare il funzionamento del quadro giuridico 2005,
- Decisione quadro 2005/222/GAI27 del Consiglio relativa agli attacchi contro i sistemi di informazione
- 2006, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni - Una strategia per una società dell'informazione sicura - "Dialogo, partenariato e responsabilizzazione" COM/2006/0251 def.
- 2013, Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi informativi e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.
- 2012, "Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo". Comitato, Piano d'azione in materia di politica industriale della sicurezza per un'industria della sicurezza innovativa e competitiva" (2012) COM/2012/0417 def.
- 2020, Comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio, La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN(2020) 18 definitivo.
 - La strategia prevede tre aree di intervento:
 - resilienza, sovranità tecnica e leadership; scudo di cibersicurezza
 - ‡ Internet degli oggetti sicuro DNS4EU
 - capacità operativa di prevenzione, dissuasione e risposta;
 - Unità congiunta di sicurezza informatica
 - cooperazione per far progredire il cyberspazio globale e aperto

La strategia dell'Unione europea per la sicurezza

La strategia copre il periodo dal 2020 al 2025 e si concentra sui settori prioritari in cui l'UE può aiutare gli Stati membri a promuovere la sicurezza per tutti coloro che vivono in Europa, nel rispetto dei nostri valori e principi europei.

- Terrorismo e criminalità
 - organizzata Criminalità
 - organizzata
 - Terrorismo e radicalizzazione
- Ambiente di sicurezza a prova di futuro
 - Infrastrutture critiche
 - Cybersecurity
 - Protezione degli spazi pubblici
- Un forte ecosistema di sicurezza
 - Rafforzare la ricerca e l'innovazione
 - Cooperazione e scambio di informazione
 - Competenze e sensibilizzazione
 - Frontiere esterne forti

- Affrontare le minacce in evoluzione
 - Minacce ibride
 - Contenuti illegali online
 - Crimine informatico
 - L'applicazione moderna della legge

Struttura di governance dell'UE

Struttura di governance dell'UE

Struttura decentralizzata

- Assegnazione alle tre diverse aree della cybersecurity: Sicurezza delle reti e delle informazioni, criminalità informatica e difesa informatica.
- ENISA
 - Istituito nel 2004, ha ricevuto un nuovo mandato permanente nel 2019 con la legge sulla sicurezza informatica dell'UE.
 - Sensibilizza e assiste l'UE, gli Stati membri e le parti interessate pubbliche e private a sviluppare e migliorare la resilienza informatica e le capacità di risposta.
 - Responsabile della preparazione degli schemi europei di certificazione della cybersecurity, che serviranno come base per la certificazione di prodotti, processi e servizi ICT.
- CERT-EU, CSIRT, Gruppo di cooperazione, Rete di CSIRT e FIRST

Cybercrime

- Centro europeo per la cibercriminalità (EC3)
 - Supporto operativo e formazione agli Stati membri ed è diventato il primo centro di competenza per le operazioni di cybercrime Cyberdefense
- Agenzia europea per la difesa (EDA) e Stato maggiore dell'UE
 - funzione consultiva, lasciando agli Stati membri le realtà operative e strategiche della difesa

L'ecosistema di sicurezza informatica dell'UE è strutturato attorno a quattro pilastri fondamentali: **resilienza, applicazione della legge, difesa cibernetica e sicurezza informatica.**

Diplomazia. Ogni pilastro coinvolge diverse organizzazioni e meccanismi dell'UE che collaborano per migliorare la sicurezza informatica in tutta l'Unione.

Sezioni e funzioni:

1. **Proteggere e sostenere i cittadini dell'UE:**
 - Si concentra sulla salvaguardia del benessere digitale dei cittadini europei.
2. **Protezione delle istituzioni, degli organi e delle agenzie dell'UE:**
 - **dell'UE:** Dedicato alla sicurezza informatica delle istituzioni dell'UE.
3. **Reti di coordinamento, meccanismi e programmi di sostegno:**
 - Si concentra sulla collaborazione tra reti e programmi per sostenere la sicurezza informatica.

L'Unità Cibernetica Congiunta supporterà i partecipanti a:

- Creare **un inventario** delle capacità operative e tecniche disponibili nell'UE;
- Produrre **relazioni integrate sulla situazione della sicurezza informatica dell'UE**, comprese informazioni e intelligence su minacce e incidenti;
- Realizzare il **piano di risposta agli incidenti e alle crisi di sicurezza informatica dell'UE**, basato sui piani nazionali proposti nella revisione della direttiva NIS (NIS2);
- Concludere **protocolli d'intesa** per la cooperazione e l'assistenza reciproca; istituire e mobilitare
- **squadre di reazione rapida per la sicurezza informatica** dell'UE;
- **Condividere informazioni e concludere accordi di cooperazione operativa.**

Condivisione delle informazioni


Più sofisticati sono gli attacchi informatici, più stretta dovrebbe essere la collaborazione tra attori pubblici e privati.

I meccanismi di condivisione delle informazioni sono


fondamentali Come deve essere inquadrato il coinvolgimento dei privati?

- La sicurezza è sempre stata una delle prerogative più importanti di uno Stato, ma la
- conoscenza tecnica del settore è per lo più nelle mani di attori privati.

I regolamenti e le direttive sono due tipi di atti giuridici dell'UE con caratteristiche distinte. Un regolamento è direttamente applicabile in tutti gli Stati membri subito dopo l'adozione, garantendo l'uniformità in quanto diventa legge senza richiedere una legislazione nazionale. Questo è l'ideale quando l'UE cerca standard coerenti, come nel caso della protezione dei dati con il GDPR. Al contrario, una direttiva stabilisce un obiettivo che gli Stati membri devono raggiungere, ma consente loro una certa flessibilità nelle modalità di attuazione. Ogni Stato membro è tenuto a recepire la direttiva nel proprio ordinamento nazionale, che può variare per adattarsi ai diversi contesti giuridici e sociali. Mentre i regolamenti sono uniformemente vincolanti in tutti i dettagli, le direttive vincolano solo per quanto riguarda il risultato, lasciando agli Stati membri la discrezionalità sui mezzi per raggiungerlo.

 Regolamento 2019/881 (legge sulla sicurezza informatica):

- **Il punto 6** fa riferimento alla necessità di una serie completa di misure di sicurezza informatica dell'UE che si basi sulle azioni precedenti e persegua obiettivi che si rafforzano a vicenda. Questi obiettivi si concentrano sull'aumento delle capacità di cybersecurity e preparazione degli Stati membri e delle imprese, rafforzando la cooperazione e la condivisione delle informazioni in tutta l'UE e potenziando le capacità a livello dell'Unione per sostenere gli Stati membri, soprattutto in caso di incidenti transfrontalieri su larga scala, e migliorando le risposte nazionali.
- **Il punto 29** affronta il ruolo dell'**ENISA** nel promuovere la cooperazione pubblico-privato e all'interno del settore privato, in particolare per proteggere le infrastrutture critiche. L'ENISA ha il compito di sostenere la condivisione delle informazioni offrendo migliori pratiche, strumenti, orientamenti procedurali e consulenza normativa, compresa la facilitazione dei centri di condivisione e analisi delle informazioni settoriali, in

 Direttiva 2022/2555 (NIS 2):

- **Il punto 41** sottolinea la necessità che gli Stati membri dispongano di sufficienti capacità tecniche e organizzative per prevenire, individuare, rispondere e mitigare gli incidenti e i rischi di cybersecurity. A tal fine, gli Stati membri dovrebbero istituire o designare uno o più Computer Security Incident Response Teams (CSIRT) e assicurarsi che siano dotati di risorse adeguate e di un buon livello tecnico. Questi CSIRT devono soddisfare i requisiti della direttiva per garantire una risposta e una cooperazione efficaci in tutta l'UE. Gli Stati membri possono designare i CERT esistenti come CSIRT. Inoltre, se un CSIRT fa parte di un'autorità competente, si dovrebbe prendere in considerazione la separazione funzionale tra i compiti operativi del CSIRT (ad esempio, la condivisione delle informazioni) e i compiti di vigilanza per rafforzare la fiducia nei confronti degli enti.
- **Il punto 119** riguarda l'importanza di condividere le informazioni sulle minacce e sulle vulnerabilità, data la crescente complessità delle minacce informatiche. La condivisione regolare delle informazioni aumenta la consapevolezza delle minacce informatiche, aiutando le entità a prevenire gli incidenti e a contenerne gli effetti, e recuperare in modo più efficace. Tuttavia, le incertezze relative alle norme sulla concorrenza e sulla responsabilità a livello di UE hanno ostacolato tale condivisione di informazioni, indicando la necessità di una guida a livello di Unione per facilitare questo processo.

Operativizzare la condivisione delle informazioni

- Le autorità pubbliche hanno cercato di migliorare la sicurezza chiedendo alle aziende private di condividere le informazioni.
- Gli attori privati si sono dimostrati riluttanti a condividere volontariamente le informazioni relative alle attività che svolgono.

Partenariati pubblico-privati

I partenariati pubblico-privati sono definiti come "un contratto a lungo termine tra una parte privata e un'entità governativa, per la fornitura di un bene o di un servizio pubblico, in cui la parte privata si assume un rischio e una responsabilità gestionale significativi, e la remunerazione è legata ai risultati" (Banca Mondiale).

- I diversi gruppi di attori coinvolti in ogni settore determineranno, in base alle caratteristiche delle loro attività, un rapporto più o meno stretto tra attori privati e pubblici.
- Gli attori che svolgono attività a livello di infrastruttura fisica hanno un rapporto marginale con le autorità del settore pubblico. Mentre i soggetti privati che forniscono servizi e prodotti ai consumatori hanno un rapporto stretto con le autorità pubbliche.

Studio ENISA sul PPP

Modelli cooperativi per il partenariato pubblico-privato (PPP)

- Fornire informazioni sui PPP in Europa attraverso la raccolta di informazioni e l'analisi dello stato attuale dei PPP e identificare i principali modelli di questo tipo di collaborazione.
- Identificare le sfide attuali che il settore pubblico e quello privato devono affrontare nel processo di creazione e sviluppo dei PPP Formulare e
- proporre raccomandazioni per lo sviluppo dei PPP in Europa

Un partenariato pubblico-privato (PPP) è un accordo/cooperazione/collaborazione a lungo termine tra due o più settori pubblici e privati e si è sviluppato nella storia in molti settori.

Il PPP non riguarda solo la cooperazione pubblico-privato. Include anche le relazioni privato-privato e pubblico-pubblico che guidano la creazione del PPP:

- Interessi economici
- Requisiti normativi Relazioni
- pubbliche
- Altri motivi

Motivazioni e vantaggi dei Partenariati Pubblico-Privato (PPP) nella cybersecurity, sottolineando come il **settore privato** e il **governo** ciascuno di essi trae vantaggio dalla collaborazione. L'obiettivo comune di entrambi i settori è quello di migliorare i livelli complessivi di sicurezza informatica.

Motivazioni e vantaggi principali:

Per il **settore privato**, i PPP consentono l'accesso ai fondi pubblici e alle conoscenze del settore, comprese le informazioni riservate. Inoltre, garantiscono la qualità dei prodotti, offrono l'opportunità di influenzare la legislazione e di definire gli standard obbligatori.

Per il **governo**, i PPP migliorano la comprensione delle esigenze del settore, creano sinergie con le iniziative private e forniscono accesso alle risorse del settore privato, allineandosi al diritto e alle normative internazionali.

Il **quadro del PPP** favorisce la fiducia, promuove la condivisione delle conoscenze, aumenta la resilienza della cybersecurity e stabilisce connessioni credibili tra le parti interessate. La comprensione del modo in cui i PPP vengono avviati ed evolvono - attraverso modelli come Top Down, Bottom Up, Fire and Forget o Split and Merge - guida lo sviluppo di nuove partnership.

Tipi di PPP

PPP istituzionali

Formati in base ad atti legali relativi alla protezione delle infrastrutture critiche, spesso coinvolgono gruppi di lavoro, squadre di pronto intervento e comunità a lungo termine.

PPP orientati agli obiettivi

Creati per costruire una cultura della cybersicurezza negli Stati membri, questi partenariati si concentrano su obiettivi specifici e fungono da piattaforme per lo scambio di conoscenze e best practice.

Outsourcing dei servizi di sicurezza informatica

Formati da governi e settori privati, questi PPP aumentano la consapevolezza della cybersicurezza e agiscono come fornitori terzi per le esigenze del settore, sostenendo al contempo la definizione e l'attuazione delle politiche.

PPP ibridi

Includere i CSIRT che operano in un quadro di PPP, con il compito di fornire servizi di cybersecurity alle amministrazioni pubbliche o a livello nazionale, come assegnato dai governi.

Sfide

Nonostante i vantaggi, i PPP devono affrontare sfide significative:

- La carenza di risorse umane qualificate sia nel settore pubblico che in quello privato.
- Bilanci e risorse pubbliche insufficienti a soddisfare le aspettative del settore privato.
- Difficoltà nello stabilire una comprensione condivisa e un dialogo tra i settori. Scarsa consapevolezza
- e promozione dei PPP tra le PMI.
- Mancanza di leadership e di quadri giuridici chiari

Organizzazione europea per la sicurezza informatica

L'ECSO è un'organizzazione no-profit di diritto belga completamente autofinanziata, istituita nel giugno 2016. È stata creata per agire come controparte della Commissione in un partenariato pubblico-privato contrattuale che copre Horizon 2020 negli anni dal 2016 al 2020. La maggioranza

dei 250 membri di ECSO appartengono all'industria della cybersecurity o a istituzioni accademiche di ricerca nel settore. In minore, i membri di ECSO comprendono anche attori del settore pubblico e industrie del lato della domanda. Oltre a formulare raccomandazioni su Horizon 2020, ECSO svolge diverse attività volte alla creazione di comunità e allo sviluppo industriale a livello europeo.

Quadro legislativo dell'UE

Legislazione UE sulla sicurezza informatica

La direttiva sulla resilienza delle infrastrutture critiche (2008) si è evoluta nella direttiva sulla resilienza delle entità critiche (2022). La direttiva NIS (2016) è stata sostituita dalla direttiva NIS 2 (2022). Altri atti legislativi fondamentali sono la legge sulla cybersecurity (2018), il regolamento sulla sicurezza informatica (2018) e il regolamento sulla sicurezza informatica (2018).

Centro di competenza e rete europea per la sicurezza informatica (2021), la legge sulla solidarietà informatica (2023), la legge sulla resilienza informatica (2024), la legge sull'intelligenza artificiale (2024) e lo spazio europeo dei dati sanitari (2024).

Centro di competenza e rete europea per la sicurezza informatica

Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro di competenza europeo per l'industria, la tecnologia e la ricerca in materia di cibersicurezza e la rete dei centri nazionali di coordinamento.

- Il Centro Europeo di Competenza per la Cybersecurity (ECCC), insieme alla Rete dei Centri Nazionali di Coordinamento (NNCC), è il nuovo quadro europeo per sostenere l'innovazione e la politica industriale in materia di cybersecurity.
- L'ECCC, che avrà sede a Bucarest, svilupperà e implementerà, insieme agli Stati membri, all'industria e al settore della cybersecurity, un sistema di sicurezza informatica. Comunità tecnologica, un'agenda comune per lo sviluppo della tecnologia e per la sua ampia diffusione in settori di interesse pubblico e nelle imprese, in particolare le PMI
- Il Centro e la Rete rafforzeranno insieme la sovranità tecnologica attraverso investimenti congiunti in progetti strategici di cybersecurity.

Il punto 16 spiega che il Centro di competenza non dovrebbe impegnarsi in compiti operativi di cybersecurity, come il monitoraggio e la gestione degli incidenti, che sono di competenza dei CSIRT. Tuttavia, può sostenere lo sviluppo di infrastrutture ICT per le industrie e le PMI, ricerca, società civile e settore pubblico. Sebbene il Centro di competenza e la Comunità di competenza per la cibersicurezza possano assistere i CSIRT nella segnalazione delle vulnerabilità, questo supporto dovrebbe rientrare nel loro ambito ed evitare di duplicare il ruolo dell'ENISA.

Il punto 17 sottolinea che il Centro di competenza, la Comunità e la Rete beneficeranno dell'esperienza acquisita grazie al partenariato pubblico-privato dell'UE con l'Organizzazione europea per la sicurezza informatica (ECSO) nell'ambito di Orizzonte 2020. Inoltre, si avvarranno degli insegnamenti tratti dai progetti pilota (CONCORDIA, ECHO, SPARTA e CyberSec4Europe) e dall'iniziativa FOSSA dell'UE per gestire e rappresentare la sicurezza informatica. Comunità in modo efficace all'interno del Centro di competenza.

Il Centro di competenza deve facilitare e coordinare il lavoro della Rete.

- La rete dovrebbe essere composta da un centro di coordinamento nazionale per ogni Stato membro.
- I centri nazionali di coordinamento che sono stati riconosciuti dalla Commissione come aventi la capacità necessaria di gestire i fondi per adempiere alla missione e agli obiettivi stabiliti nel presente regolamento dovrebbero ricevere il sostegno finanziario diretto dell'Unione, comprese le sovvenzioni concesse senza invito a presentare proposte, al fine di svolgere le loro attività in relazione al presente regolamento.
- I centri di coordinamento nazionali dovrebbero essere enti del settore pubblico, o enti a maggioranza pubblica, che svolgono funzioni di pubblica amministrazione ai sensi del diritto nazionale, anche mediante delega, e dovrebbero essere selezionati dagli Stati membri.
- I centri di coordinamento nazionali devono avere la necessaria capacità amministrativa, devono possedere o avere accesso a competenze industriali, tecnologiche e di ricerca in materia di cybersecurity e devono essere in grado di impegnarsi e coordinarsi efficacemente con l'industria, il settore pubblico e la comunità di ricerca.

Direttiva sulla resilienza delle entità critiche

Direttiva (UE) 2022/2557 sulla resilienza delle entità critiche

La **direttiva sulle infrastrutture critiche europee (ECI)** del 2008 si applica solo ai settori dell'energia e dei trasporti e prevede un processo per l'identificazione e la designazione delle ECI la cui interruzione avrebbe un impatto su almeno due Stati membri. Stabilisce i requisiti di protezione per le ECI operatori e autorità nazionali competenti. Finora sono state designate 94 ICE, soprattutto nel settore dell'energia e concentrate in alcuni Paesi dell'Europa centrale e orientale. Tuttavia, gli sforzi dell'UE per la resilienza delle infrastrutture critiche comprendono anche azioni settoriali e intersettoriali più ampie, tra cui la protezione del clima, la protezione civile, gli investimenti diretti esteri e la sicurezza informatica. Inoltre, gli Stati membri hanno attuato misure diverse in questo settore.

Direttiva sulla resilienza delle entità critiche

L'attuale panorama dei rischi per le infrastrutture critiche è diventato più complesso dal 2008, coinvolgendo ora rischi naturali aggravati dal clima, minacce ibride sponsorizzate dallo Stato, terrorismo, minacce interne, pandemie e incidenti industriali. Gli operatori si trovano ad affrontare sfide nell'adozione di tecnologie come il 5G e i veicoli senza pilota, che portano sia vantaggi operativi che nuove vulnerabilità. Aumento

L'interdipendenza tra i settori significa che le perturbazioni in un settore possono innescare effetti a cascata in altri, con potenziali ripercussioni su più Stati membri o sull'intera UE. L'ambito di applicazione copre ora dieci settori, tra cui l'energia, i trasporti, la finanza, la sanità, le infrastrutture digitali e lo spazio. Gli Stati membri sono tenuti a identificare le entità critiche sulla base di valutazioni nazionali del rischio e ad applicare le norme di sicurezza. obblighi, soprattutto per le entità di rilevanza europea che forniscono servizi essenziali in più Stati membri.

I principali cambiamenti nella politica delle infrastrutture critiche sottolineano il passaggio dalla **protezione alla resilienza**. Mentre la protezione si concentra sulla prevenzione degli incidenti attraverso la valutazione del rischio, la resilienza accetta che gli incidenti si verifichino e incorpora sia la prevenzione che la risposta. misure. Non esistono standard consolidati per valutare efficacemente la resilienza.

L'ambito di applicazione si è inoltre spostato dalle **Infrastrutture Critiche Europee alle Entità Critiche**, adottando un approccio più bottom-up e basato su agenti. La politica copre ora una gamma più ampia di **11 settori critici** (tra cui energia, trasporti e altri) e riconosce le crescenti interdipendenze tra settori, Paesi e sistemi fisico-digitali.

L'approccio politico si è ampliato, passando da un'attenzione prioritaria per il terrorismo a un **approccio a tutto campo**, che affronta vari rischi.

Per quanto riguarda il **coordinamento della cybersecurity**, il nuovo approccio si allinea alla direttiva NIS 2, che migliora la resilienza delle entità "essenziali" e "importanti" in tutti i settori. Le autorità competenti per le entità critiche e quelle per la NIS 2 collaboreranno per garantire la resilienza. contro i rischi informatici e non informatici. Le entità critiche ai sensi della NIS 2 hanno obblighi più ampi di gestione dei rischi non informatici e la sicurezza fisica dell'infrastruttura digitale è integrata nella gestione del rischio di cybersecurity e nella rendicontazione ai sensi della NIS 2.

Direttiva NIS

Direttiva UE 2016/1148 relativa alle misure per un elevato livello di sicurezza comune dei sistemi di rete e d'informazione in tutta l'Unione Art. 1(1): La presente direttiva stabilisce misure al fine di conseguire un elevato livello comune di sicurezza dei sistemi di rete e dei sistemi informativi nell'Unione, in modo da migliorare il funzionamento del mercato interno

Articolo 1, paragrafo 7: Qualora un atto giuridico dell'Unione specifico del settore imponga agli operatori di servizi essenziali o ai fornitori di servizi digitali di garantire la sicurezza della loro rete e dei loro sistemi informativi o di notificare incidenti, purché tali requisiti abbiano un effetto almeno equivalente agli obblighi stabiliti nella presente direttiva, si applicano le disposizioni di tale atto giuridico dell'Unione specifico del settore.

Obiettivi

Questo paragrafo analizza le sfide della cybersicurezza nell'Unione Europea, evidenziando alcune questioni chiave:

1. Le attuali capacità di cybersecurity sono inadeguate a garantire una sicurezza di alto livello delle reti e dei sistemi informativi in tutta l'UE.
2. C'è una significativa disparità nei livelli di preparazione tra gli Stati membri, che porta a: approcci
 - frammentati
 - Protezione disomogenea per consumatori e imprese Livelli di sicurezza
 - complessivi compromessi in tutta l'Unione
3. Vengono identificati due problemi principali:
 - Mancanza di requisiti comuni per gli operatori di servizi essenziali
 - Mancanza di requisiti comuni per i fornitori di servizi digitali
4. Queste lacune rendono impossibile l'istituzione di un efficace meccanismo di cooperazione a livello europeo.
5. Il paragrafo conclude sottolineando il ruolo cruciale che le istituzioni accademiche (università e centri di ricerca) svolgono nel promuovere la ricerca, lo sviluppo e l'innovazione in queste aree.

Il tema centrale è che la frammentazione e la mancanza di standardizzazione delle misure di cybersicurezza negli Stati membri dell'UE ostacolano una protezione efficace a livello dell'Unione.

Obiettivi della direttiva NIS

- **Cooperazione a livello di Unione:** È prevista l'istituzione di un gruppo di cooperazione a livello dell'Unione per agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri. Inoltre, verrà creata una rete di Computer Security Incident Response Teams (CSIRTs) per promuovere la cooperazione operativa.
- **Strategia nazionale e autorità competenti:** Gli Stati membri devono adottare una strategia nazionale per la sicurezza delle reti e delle informazioni e designare le autorità nazionali competenti. Ogni Stato membro deve inoltre designare almeno un CSIRT competente per i servizi essenziali.
- **Conformità da parte di operatori e fornitori:** Gli operatori di servizi essenziali (OES) e i fornitori di servizi digitali (DSP) sono tenuti a rispettare i requisiti di sicurezza stabiliti.

Quadri nazionali

Articolo 7: Strategia nazionale sulla sicurezza delle reti e dei sistemi informativi

1. **Requisito della strategia nazionale:** Ogni Stato membro deve adottare una strategia nazionale per garantire la sicurezza delle reti e dei sistemi informativi. La strategia deve delineare gli obiettivi strategici, le politiche e le misure per mantenere elevati livelli di sicurezza nei settori elencati nell'allegato II e nei servizi dell'allegato III. Essa deve riguardare i seguenti punti chiave:
 - Obiettivi e priorità per la sicurezza delle reti e delle informazioni.
 - Quadro di governance, che definisce ruoli e responsabilità degli enti governativi e degli attori rilevanti. Misure per la preparazione, la risposta e il recupero, compresa la cooperazione pubblico-privato.
 - Programmi di educazione, sensibilizzazione e formazione in materia di sicurezza. Piani di ricerca e sviluppo per la sicurezza delle reti e delle informazioni. Un piano di valutazione dei rischi per identificare i potenziali rischi per la sicurezza.
 - Un elenco degli stakeholder coinvolti nell'attuazione della strategia.
2. **Assistenza dell'ENISA:** Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo delle loro strategie nazionali.

Articolo 9: Gruppi di risposta agli incidenti di sicurezza informatica (CSIRT)

1. **Designazione dei CSIRT:** Ogni Stato membro deve designare uno o più CSIRT responsabili della gestione dei rischi e degli incidenti, garantendo che coprano i settori e i servizi specificati negli allegati II e III. I CSIRT devono seguire un processo ben definito e possono essere istituiti all'interno di un'autorità competente.
2. **Assegnazione delle risorse:** Gli Stati membri devono garantire che i CSIRT dispongano di risorse adeguate per svolgere efficacemente i loro compiti, come indicato nell'Allegato I. Devono inoltre assicurare una cooperazione sicura ed efficiente all'interno della rete CSIRT (articolo 12).
3. **Infrastruttura:** Gli Stati membri devono garantire che i CSIRT abbiano accesso a un'infrastruttura di comunicazione sicura e resiliente a livello nazionale.
4. **Competenze dei CSIRT:** Gli Stati membri devono informare la Commissione sulle competenze e sugli elementi chiave dei processi di gestione degli incidenti dei loro CSIRT.
5. **Assistenza dell'ENISA:** Gli Stati membri possono richiedere l'assistenza dell'ENISA per lo sviluppo di CSIRT

nazionali. Target ☐ Operatori di servizi essenziali e fornitori di servizi digitali

Operatori di servizi essenziali

Art 5)

1. Entro il 9 novembre 2018, per ciascun settore e sottosettore di cui all'allegato II, gli Stati membri individuano gli operatori di servizi essenziali con uno stabilimento nel loro territorio.
2. I criteri per l'identificazione degli operatori di servizi essenziali, di cui al punto (4) dell'articolo 4, sono i seguenti:
 - a. Un'entità fornisce un servizio essenziale per il mantenimento di attività sociali e/o economiche critiche.
 - b. La fornitura di questo servizio dipende dai sistemi di rete e di informazione.
 - c. Un incidente avrebbe *effetti di disturbo significativi* sulla fornitura di tale servizio

Incidenti critici

Art 6) Significativo effetto dirompente

1. Nel determinare la rilevanza di un effetto dirompente di cui all'articolo 5, paragrafo 2, lettera c), gli Stati membri tengono conto almeno dei seguenti fattori intersettoriali:
 - a. Il numero di utenti che si affidano al servizio fornito dall'ente in questione;
 - b. La dipendenza di altri settori di cui all'Allegato II dal servizio fornito da tale entità;
 - c. L'impatto che gli incidenti potrebbero avere, in termini di grado e durata, sulle attività economiche e sociali o sulla sicurezza pubblica;
 - d. La quota di mercato di tale entità;
 - e. La diffusione geografica dell'area che potrebbe essere interessata da un incidente;
 - f. L'importanza dell'entità per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di mezzi alternativi per la fornitura di tale servizio.

Operatori di servizi essenziali

Approccio coerente nell'identificazione delle OES

1. Ridurre i rischi legati alle dipendenze transfrontaliere;
2. Garantire condizioni di parità per gli operatori nel mercato interno;
3. Ridurre il rischio di interpretazioni divergenti della direttiva;
4. Sviluppare una panoramica completa del livello di resilienza informatica nell'UE.

Requisiti di sicurezza - OSE

Art 14 Requisiti di sicurezza e notifica degli incidenti

1. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza delle reti e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto dello stato dell'arte, tali misure devono garantire un livello di sicurezza dei sistemi di rete e di informazione adeguato al rischio che essi comportano.
2. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure adeguate per prevenire e ridurre al minimo l'impatto di incidenti che incidono sulla sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di garantire la continuità di tali servizi.

Notifica dell'incidente - OSE

Art 14 Requisiti di sicurezza e notifica degli incidenti

3. Gli Stati membri assicurano che gli operatori di servizi essenziali notifichino, senza indebito ritardo, all'autorità competente o al CSIRT gli incidenti che hanno un impatto significativo sulla continuità dei servizi essenziali che forniscono. Le notifiche includono informazioni che consentano all'autorità competente o al CSIRT di determinare l'eventuale impatto transfrontaliero dell'incidente. La notifica non comporta una maggiore responsabilità per la parte notificante.
4. Per determinare la significatività dell'impatto di un incidente, devono essere presi in in particolare i seguenti parametri:
 - a. Il numero di utenti interessati dall'interruzione del servizio essenziale;
 - b. La durata dell'incidente;
 - c. La distribuzione geografica rispetto all'area interessata dall'incidente.

Notifica al pubblico

Le autorità competenti dovrebbero dare priorità al mantenimento di canali informali e fidati per la condivisione delle informazioni. Quando vengono segnalati gli incidenti, essi devono bilanciare l'interesse del pubblico a essere informato con i potenziali rischi commerciali e di reputazione per gli operatori dei servizi essenziali. Inoltre, le autorità e i CSIRT devono garantire che le informazioni sulle vulnerabilità dei prodotti rimangano riservate fino al rilascio delle opportune correzioni di sicurezza.

Fornitori di servizi digitali

Molte imprese dell'Unione dipendono da fornitori di servizi digitali, i cui servizi sono fondamentali per il buon funzionamento di varie operazioni, comprese quelle degli operatori di servizi essenziali. Dal momento che le interruzioni di questi servizi digitali possono avere un impatto sulle principali attività economiche e

La presente direttiva si applica ai fornitori che offrono tali servizi digitali essenziali. Questi fornitori svolgono un ruolo fondamentale nel garantire la continuità delle attività, la partecipazione al mercato interno e il commercio transfrontaliero all'interno dell'Unione.

Requisiti di sicurezza - DSP

L'articolo 16 definisce i requisiti di sicurezza e gli obblighi di notifica degli incidenti per i fornitori di servizi digitali:

1. **Misure di sicurezza:** Gli Stati membri devono garantire che i fornitori di servizi digitali mettano in atto misure tecniche e organizzative adeguate per gestire i rischi di sicurezza legati alla loro rete e ai loro sistemi informativi. Tali misure devono essere proporzionate al rischio e considerare la sicurezza del sistema, la gestione degli incidenti, la continuità operativa, il monitoraggio, l'audit e gli standard internazionali.
2. **Mitigazione del rischio:** I fornitori devono adottare misure per prevenire e ridurre al minimo l'impatto degli incidenti sui servizi offerti, garantendo la continuità di tali servizi.
3. **Notifica degli incidenti:** I fornitori devono notificare immediatamente all'autorità competente o al CSIRT se un incidente ha un impatto significativo sulla fornitura di servizi. La notifica deve aiutare a valutare l'eventuale impatto transfrontaliero, ma non aumenta la responsabilità della parte notificante.
4. **Valutazione dell'impatto:** Nel determinare se un incidente è sostanziale, si devono fattori quali il numero di utenti colpiti, la durata, la diffusione geografica, l'interruzione del servizio e l'impatto sulle attività economiche e sociali. Gli obblighi di notifica si applicano solo se il provider è in grado di valutare l'impatto dell'incidente sulla base di questi parametri.

Un approccio diverso al DSP

I fornitori di servizi digitali devono garantire misure di sicurezza adeguate ai rischi che i loro servizi comportano, considerando la loro importanza per le altre imprese. Poiché gli operatori di servizi essenziali devono affrontare rischi più elevati a causa del loro ruolo critico, i fornitori di servizi digitali hanno requisiti di sicurezza più leggeri. Possono implementare le misure che ritengono adatte a gestire i rischi, ma data la loro natura transfrontaliera, dovrebbero seguire un approccio più unificato a livello dell'Unione. Gli atti di esecuzione contribuiranno a definire e guidare queste misure di sicurezza.

Valutazione NIS

Ampio e astratto: pro e contro

Test e controlli uniformi e continui non sono obbligatori
Ruolo limitato delle autorità di polizia

La direttiva (UE) 2022/2555 (NIS 2) amplia l'ambito di applicazione della precedente direttiva NIS per includere nuovi settori critici per l'economia e la società. Elimina la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali. Inoltre, rafforza i requisiti di sicurezza introducendo un approccio di gestione del rischio, garantendo che le aziende adottino misure appropriate per gestire e mitigare efficacemente i rischi di cybersecurity.

Direttiva NIS 2

- **Medie imprese:** La direttiva si applica alle entità pubbliche o private elencate nell'allegato I o II che si qualificano come medie imprese. imprese secondo i criteri di cui all'articolo 2 dell'allegato alla raccomandazione 2003/361/CE, o superano tali soglie dimensionali e operano all'interno dell'Unione. L'eccezione all'articolo 3, paragrafo 4, di tale raccomandazione si applica ai fini della presente direttiva.
- **Enti che forniscono servizi critici:** La direttiva si applica anche alle entità dei tipi elencati nell'allegato I o II, indipendentemente dalle loro dimensioni, se soddisfano una o più delle seguenti condizioni:
 - Fornire servizi quali comunicazioni elettroniche pubbliche, servizi fiduciari o servizi di nomi di dominio.
 - Sono l'unico fornitore in uno Stato membro di un servizio fondamentale per il mantenimento delle attività sociali o economiche.
 - L'interruzione del servizio potrebbe avere un impatto significativo sulla sicurezza, l'incolumità o la salute pubblica.
 - L'interruzione del servizio potrebbe comportare rischi sistemici, in particolare con impatti transfrontalieri.
 - Sono critici per la loro specifica importanza a nazionale o regionale, o all'interno di settori interconnessi.
 - Si tratta di enti della pubblica amministrazione a livello di governo centrale o regionale, che forniscono servizi la cui interruzione potrebbe avere gravi ripercussioni sulle attività sociali o economiche.
- **Entità critiche:** La direttiva si applica alle entità identificate come critiche ai sensi della **direttiva (UE) 2022/2557**, indipendentemente dalle loro dimensioni.
- **Servizi di registrazione di nomi di dominio:** La direttiva si applica alle entità che forniscono servizi di registrazione di nomi di dominio, indipendentemente dalle loro dimensioni.

Requisiti di sicurezza

- **Requisiti di gestione del rischio:** Gli Stati membri devono garantire che le entità essenziali e importanti implementino misure tecniche, operative e organizzative appropriate per gestire i rischi per la sicurezza della loro rete e dei loro sistemi informativi. Queste misure devono prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei servizi e sugli altri servizi. Le misure devono essere proporzionate ai rischi posti, considerando l'esposizione dell'ente ai rischi, le dimensioni e la potenziale gravità degli incidenti, compresi gli impatti sociali ed economici.
- **Approccio all-hazards:** Le misure di gestione del rischio devono adottare un approccio all-hazards per proteggere i sistemi di rete e informativi e i loro ambienti fisici. Tali misure devono includere, come minimo
 - Analisi dei rischi e politiche di sicurezza dei sistemi informativi.
 - Procedure di gestione degli incidenti.
 - Misure di continuità aziendale, come la gestione dei backup e la gestione delle crisi.
 - Sicurezza della catena di approvvigionamento, con particolare attenzione ai rapporti con i fornitori e i prestatori di servizi.
 - Sicurezza nell'acquisizione, nello sviluppo, nella manutenzione e nella gestione delle vulnerabilità dei sistemi.
 - Politiche di valutazione dell'efficacia delle misure di cybersecurity.
 - Pratiche di igiene informatica e formazione sulla cybersicurezza.
 - Crittografia e politiche di crittografia.
 - Sicurezza delle risorse umane, controllo degli accessi e gestione degli asset.

o Utilizzo di autenticazione a più fattori o continua, di sistemi di comunicazione protetti e di soluzioni di comunicazione di emergenza, secondo le necessità.

Notifica degli incidenti

1. **Notifica degli incidenti:** Gli Stati membri devono garantire che le entità essenziali e importanti notifichino al loro CSIRT o all'autorità competente senza indugio su incidenti significativi che incidono sulla fornitura dei loro servizi. Le entità devono inoltre informare i destinatari dei servizi se è probabile che l'incidente li riguardi. La notifica deve includere informazioni che consentano al CSIRT o all'autorità competente di valutare qualsiasi impatto transfrontaliero. L'atto di notifica non aumenta la responsabilità dell'ente. Se un ente notifica all'autorità competente, questa deve trasmettere le informazioni al CSIRT. Per gli incidenti transfrontalieri o intersettoriali, gli Stati membri devono garantire la condivisione tempestiva delle informazioni con i contatti pertinenti.
2. **Comunicazione con i destinatari del servizio:** Se applicabile, gli Stati membri devono garantire che gli enti comunichino con i destinatari dei servizi. I destinatari sulle minacce informatiche significative, consigliando loro le misure che possono adottare per affrontare la minaccia. Le entità devono anche informare i destinatari della minaccia stessa, quando opportuno.
3. Un incidente è considerato significativo se:
 - (a) Provoca o potrebbe provocare gravi interruzioni operative o perdite finanziarie per l'entità.
 - (b) Colpisce o potrebbe colpire altri individui o entità, causando notevoli danni materiali o non materiali.
4. **Obblighi di segnalazione:** Gli Stati membri devono garantire che gli enti segnalino gli incidenti significativi al CSIRT o all'autorità competente entro i termini stabiliti:
 - **Allarme preventivo (entro 24 ore):** L'ente deve fornire un allarme tempestivo, specificando se si sospetta che l'incidente sia causato da atti illeciti o possa avere un impatto transfrontaliero.
 - **Notifica dell'incidente (entro 72 ore):** L'ente deve inviare una notifica di incidente, aggiornando l'allarme preventivo e fornendo una valutazione iniziale della gravità dell'incidente, dell'impatto e degli indicatori di compromissione.
 - **Rapporto intermedio (su richiesta):** L'ente deve fornire un aggiornamento dello stato se richiesto dal CSIRT o dall'autorità competente.
 - **Relazione finale (entro un mese):** Entro un mese deve essere consegnato un rapporto finale dettagliato che comprenda:
 - o Descrizione dettagliata dell'incidente, gravità e impatto.
 - o Tipo di minaccia probabile o causa principale.
 - o Misure di mitigazione.
 - o Impatto transfrontaliero, se applicabile.
 - Se l'incidente è in corso al momento del rapporto finale, è richiesto un rapporto sullo stato di avanzamento, con un rapporto finale entro un mese dalla risoluzione dell'incidente.

Fornitori di servizi fiduciari: Per gli incidenti significativi che riguardano i servizi fiduciari, la notifica deve essere effettuata entro 24 ore dal momento in cui se ne viene a conoscenza, invece delle consuete 72 ore.

Supervisione - entità essenziali

- **Efficacia e proporzionalità:** Gli Stati membri devono garantire che le misure di vigilanza e di esecuzione imposte ai soggetti essenziali siano efficaci, proporzionate e dissuasive, tenendo conto delle specificità di ciascun caso.
- **Poteri di vigilanza:** Le autorità competenti devono avere il potere di sottoporre gli enti essenziali a:
 - o **Ispezioni in loco e supervisione fuori sede**, compresi controlli casuali da parte di professionisti qualificati.
 - o **Audit di sicurezza regolari e mirati** effettuati da organismi indipendenti o autorità competenti.
 - o **Audit ad hoc** a seguito di incidenti significativi o violazioni della direttiva.
 - o **Scansioni di sicurezza** basate su valutazioni del rischio obiettive, non discriminatorie e trasparenti, con la collaborazione dell'ente, ove necessario.
 - o **Richieste di informazioni** per valutare le misure di gestione del rischio di cybersecurity, comprese le politiche e la conformità agli obblighi di segnalazione.
 - o **Richieste di accesso a dati, documenti e prove** necessarie per le attività di supervisione.

I controlli di sicurezza mirati devono essere basati su valutazioni del rischio e i loro risultati devono essere condivisi con l'autorità competente. I costi degli audit eseguiti da un organismo indipendente sono generalmente a carico dell'entità sottoposta ad audit, a meno che l'autorità competente non decida diversamente in casi giustificati.

Vigilanza - entità importanti

- **Misure di vigilanza ex post:** Se vi sono prove o informazioni che suggeriscono che un'entità importante non rispetta la direttiva (in particolare gli articoli 21 e 23), gli Stati membri devono assicurare che le autorità competenti prendano provvedimenti attraverso misure di vigilanza ex post. Tali misure devono essere efficaci, proporzionate e dissuasive, considerando le circostanze di ciascun caso.
- **Poteri di vigilanza:** Le autorità competenti devono avere il potere di assoggettare le entità importanti a:
 - **Ispezioni in loco e supervisione fuori sede** condotte da professionisti qualificati.
 - **Audit di sicurezza mirati** effettuati da un organismo indipendente o da un'autorità competente.
 - **Scansioni di sicurezza** basate su criteri di valutazione del rischio oggettivi, non discriminatori e trasparenti, con la collaborazione dell'ente, ove necessario.
 - **Richieste di informazioni** per valutare le misure di gestione del rischio di cybersecurity dell'ente e la conformità agli obblighi di segnalazione.
 - **Richieste di accesso a dati, documenti e informazioni** necessarie per i compiti di supervisione.
 - **Richieste di prove** dell'attuazione delle politiche di cybersecurity, come i risultati di audit di sicurezza da parte di revisori qualificati.

I controlli di sicurezza mirati devono essere basati su valutazioni del rischio e i loro risultati devono essere messi a disposizione dell'autorità competente. I costi degli audit indipendenti sono generalmente a carico dell'entità sottoposta ad audit, a meno che l'autorità competente non decida diversamente in casi specifici.

Sanzioni

Condizioni generali per l'imposizione di sanzioni amministrative a enti essenziali e importanti

1. **Sanzioni efficaci, proporzionate e dissuasive:** Gli Stati membri devono garantire che le sanzioni amministrative imposte per le violazioni della direttiva siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze specifiche di ciascun caso.
2. **In aggiunta ad altre misure:** Le ammende amministrative vengono comminate in aggiunta alle misure descritte negli articoli 32 e 33, tra cui ispezioni, audit e scansioni di sicurezza.
3. **Criteri per l'imposizione di multe:** Nel decidere se imporre un'ammenda e nel determinarne l'importo, le autorità competenti devono considerare almeno gli elementi previsti dall'articolo 32, paragrafo 7, che include fattori quali la gravità dell'infrazione.
4. **Ammende per le entità essenziali:** Le entità essenziali che violano gli articoli 21 o 23 sono soggette a sanzioni amministrative pecuniarie fino a **EUR 10.000.000** o il **2% del fatturato mondiale totale annuo** dell'impresa a cui appartiene l'entità (se superiore).
5. **Multe per le entità importanti:** Le entità importanti che violano gli articoli 21 o 23 sono soggette a sanzioni amministrative pecuniarie fino a un massimo di **euro. 7.000.000** o l'**1,4% del fatturato mondiale totale annuo** dell'impresa a cui appartiene l'entità (se superiore).

Dalla direttiva NIS all'attuazione italiana

Quadro giuridico esistente

Decreto Legislativo n. 82 del 2005 (Codice dell'Amministrazione Digitale)

- Art. 51: intervento iniziale sulla sicurezza dei dati

Legge n. 144/2005 sulle misure urgenti per il contrasto del terrorismo internazionale

- Art. Art. 7a sulla sicurezza informatica: i servizi di protezione informatica delle infrastrutture digitali critiche di interesse nazionale sono stati assegnati al Ministero dell'Interno.

Legge n. 134/2012 sull'Agenda digitale italiana

- Creazione dell'«Agenzia per l'Italia Digitale» che coordina le azioni nel campo dell'innovazione per promuovere le tecnologie ICT a supporto delle pubbliche amministrazioni, garantendo la realizzazione degli obiettivi dell'«Agenda Digitale Italiana, in coerenza con l'«Agenda Digitale Europea. Ordine del giorno

Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 sulla protezione cibernetica e la sicurezza informatica nazionale.

- Coordinamento delle attività legate alla cybersecurity che coinvolgono le amministrazioni pubbliche e la comunità di intelligence

Quadro strategico nazionale per la sicurezza del cyberspazio e Piano nazionale per il cyberspazio e la cybersecurity

- Organizzazione interna per consentire risposte tempestive e coordinate alle minacce informatiche che colpiscono i beni nazionali.

Serie di interventi

- Decreto Legislativo 65/2018:

Il Decreto Legislativo 18 maggio 2018, n. 65, attua la Direttiva UE 2016/1148 per migliorare la sicurezza delle reti e delle informazioni in tutta l'Unione Europea. I punti chiave includono:

◦ **Obiettivo (articolo 1):** Stabilire un livello elevato di sicurezza per le reti e i sistemi informativi a livello nazionale, contribuendo alla sicurezza dell'intera UE.

◦ **Segnalazione degli incidenti (articoli 12 e 14):** Gli operatori dei servizi essenziali (OES) e i fornitori di servizi digitali (DSP) sono tenuti a segnalare gli incidenti al CSIRT, mentre per le altre entità la segnalazione è facoltativa.

◦ **Sanzioni per la non conformità (articolo 21):**

- La mancata implementazione di adeguate misure di sicurezza tecniche e organizzative da parte di OES o DSP può portare a multe da 9.000 euro fino a €120.000.
- Se l'OES o il DSP non notificano al CSIRT italiano incidenti significativi, le multe vanno da 25.000 a 125.000 euro.
- Gli OES che si affidano a DSP terzi per i servizi critici rischiano multe da 12.000 a 120.000 euro se non segnalano gli incidenti Decreto

• **Legge 105/2019 (Legge 133/2019):**

Il **Perimetro Nazionale di Cybersecurity (PSNC)** in Italia estende le misure di cybersecurity al di là della Direttiva NIS dell'UE per includere enti pubblici e privati essenziali per la sicurezza nazionale. L'obiettivo è quello di proteggere le reti, i sistemi informativi e i servizi IT per le principali entità nazionali. Gli standard sono fissati per ridurre al minimo i rischi e il D.P.C.M. 131/2020 definisce i criteri per includere le entità in base alle funzioni e ai servizi essenziali.

• **DPCM 131/2020**

Le **Funzioni Essenziali** del Perimetro Nazionale di Cybersecurity italiano includono il mantenimento della continuità del governo, della difesa dello Stato, della sicurezza pubblica, della giustizia, dei sistemi economici e dei trasporti (art. 2).

I **servizi essenziali** riguardano attività critiche per le funzioni dello Stato, la tutela dei diritti, la continuità delle forniture, le infrastrutture, la logistica, i settori ad alta tecnologia e tutti i settori vitali per l'autonomia nazionale, la competitività e lo sviluppo economico.

Il perimetro di sicurezza informatica si applica alle reti, ai sistemi e ai servizi informatici in cui le interruzioni potrebbero minacciare la sicurezza

• **nazionale. DPCM 81/2021**

Le entità all'interno del **Perimetro Nazionale di Cybersecurity** italiano devono impegnarsi nella **prevenzione** e nella **notifica e risposta agli incidenti**.

Procedura:

- Le entità ricevono una notifica di inclusione nel perimetro e devono preparare un elenco delle loro reti, sistemi e servizi IT entro sei mesi, aggiornandolo annualmente.
- Devono condurre valutazioni del rischio sugli asset ICT, valutare l'impatto delle interruzioni e adottare misure di mitigazione seguendo gli standard europei e internazionali, in particolare il quadro di cybersecurity del NIST.

Notifica dell'incidente:

- Gli incidenti sono classificati in base alla gravità, con scadenze di notifica basate sul livello di gravità. Le segnalazioni vengono inviate al CSIRT italiano e la non conformità può comportare sanzioni significative.

• **Decreto presidenziale 54/2021**

Le entità all'interno del **Perimetro Nazionale di Cybersecurity** italiano devono informare il **Centro Nazionale di Valutazione e Certificazione (CVCN)** di qualsiasi prodotto o servizio ICT esternalizzato.

- **Ruolo del CVCN:** Il CVCN valuta la sicurezza dei beni, dei sistemi e dei servizi TIC destinati all'uso all'interno del perimetro, come indicato nel decreto del 15 giugno 2021.
- **Requisiti di notifica:** Le entità che pianificano l'acquisizione di prodotti TIC per aree strategiche devono presentare una notifica dettagliata al CVCN, che comprenda l'uso del prodotto, la categoria, le misure di sicurezza e l'analisi dei rischi.

◦ **Processo:**

- Il CVCN risponde con linee guida entro 60 giorni.
- I test richiesti su hardware e software vengono condotti presso le strutture del CVCN o in luoghi accreditati. Il CVCN
- fornisce i risultati della valutazione della sicurezza e le linee guida per l'utilizzo.

• **Decr. Legge 82/2021**

Il **Sistema Nazionale di Cybersecurity** dell'Italia è governato dall'**Autorità Italiana per la Cybersecurity (ACN)**, un'agenzia indipendente responsabile delle funzioni tecniche di cybersecurity.

- **ACN:** Funziona con autonomia amministrativa e finanziaria, svolgendo compiti specializzati con limitata influenza politica. salvaguardia dei diritti fondamentali. L'ACN è diretto dal **Presidente del Consiglio** e monitorato dal **COPASIR** (Comitato parlamentare di sicurezza).

◦ **Struttura di governance:**

- Il **Presidente del Consiglio** guida la strategia nazionale di cybersecurity e supervisiona l'ACN.
- **ACN** gestisce gli aspetti tecnici della sicurezza informatica.
- Il **Comitato interministeriale per la cibersicurezza (CIC)** fornisce indicazioni politiche, consulenza e supervisione sulle politiche di cibersicurezza.

Autorità italiana per la sicurezza informatica

L'**Agenzia Italiana per la Cybersecurity (ACN)** è un ente amministrativo autonomo responsabile degli sforzi di cybersecurity a livello nazionale.

- **Struttura e autonomia:** L'ACN opera con indipendenza amministrativa e finanziaria, ma è soggetta alle direttive del **Presidente del Consiglio** e alla supervisione del **COPASIR** per garantire l'imparzialità politica, soprattutto nella tutela dei diritti fondamentali.
- **Obiettivi:** Salvaguardare gli interessi nazionali in materia di sicurezza informatica, sviluppando capacità di prevenzione, monitoraggio, rilevamento e risposta alle minacce informatiche.
- **Compiti principali:**
 - Elaborare la strategia nazionale di cibersicurezza e coordinare le attività del settore pubblico e privato.
 - Migliorare la sicurezza dell'industria digitale, comprese le certificazioni per prodotti e sistemi.
 - Fornire pareri consultivi sulle misure legislative per mantenere un quadro nazionale coerente di cibersicurezza.
 - Coordinare la cooperazione europea e internazionale in materia di sicurezza informatica.
 - Sostenere la ricerca, l'innovazione e lo sviluppo di competenze nel campo della sicurezza informatica.
 - Ispezionare e far rispettare la conformità alla sicurezza informatica all'interno del **perimetro nazionale di sicurezza informatica (PSNC)**.
- **Ruolo:** Funziona come autorità di vigilanza nazionale, **CSIRT-Italia**, contatto centrale per la sicurezza delle reti, autorità di certificazione nazionale e **Centro nazionale di valutazione e certificazione (CVCN)**.

CSIRT italiano

Compiti:

- **Monitoraggio degli incidenti:** Monitoraggio degli incidenti di cibersicurezza a livello nazionale.
- **Allarmi e condivisione delle informazioni:** Emissione di pre-allarmi, avvisi e aggiornamenti sui rischi e le vulnerabilità, comprese le pubblicazioni sul sito web delle nuove minacce.
- **Risposta agli incidenti:** Intervenire attivamente negli incidenti di cybersecurity.
- **Analisi del rischio:** Conduzione di valutazioni dinamiche dei rischi e degli incidenti.
- **Consapevolezza della situazione:** Mantenere una visione d'insieme del panorama nazionale della sicurezza informatica.
- **Collaborazione internazionale:** Partecipazione alla rete CSIRT, collaborazione con **ENISA** (Agenzia dell'Unione Europea per la sicurezza informatica).

Attuazione della direttiva NIS 2

Il **Decreto Legislativo n. 138 del 4 settembre 2024** attua la Direttiva UE 2022/2555, stabilendo standard di cybersecurity in tutta l'UE e sostituendo la precedente Direttiva NIS.

- **Identificazione delle entità essenziali e importanti:** L'ACN compilerà un elenco delle aziende e delle amministrazioni pubbliche coinvolte entro aprile 2025. Tutte le entità devono registrarsi sulla piattaforma dell'ACN.
- **Obblighi di sicurezza:** L'ACN definirà requisiti di sicurezza specifici in base all'esposizione al rischio, alle dimensioni dell'entità, alla probabilità di incidenti e alla gravità dell'impatto.
- **Sanzioni:**
 - Le sanzioni variano in base al tipo di violazione, tra cui la non conformità, la mancata notifica o la mancata registrazione.
 - Per le **entità essenziali (EE)**: multe fino a 10 milioni di euro o al 2% del fatturato globale annuo.
 - Per le **entità importanti (IE)**: multe fino a 7 milioni di euro o all'1,4% del fatturato globale.
 - Multe aggiuntive per mancata registrazione e comunicazione, con un tetto massimo dello 0,1% per gli EE e dello 0,07% per gli IE.
 - Le violazioni ripetute possono triplicare le multe, e ignorare gli avvisi dell'ACN può portare alla sospensione delle certificazioni o delle autorizzazioni.

Atto di sicurezza informatica dell'UE

Il **regolamento (UE) 2019/881** (legge sulla cibersicurezza) istituisce l'**ENISA** (Agenzia dell'Unione europea per la cibersicurezza) e si concentra sulla certificazione della cibersicurezza delle TIC. Si occupa di tre fattori chiave:

1. **Leadership globale:** Puntare a far sì che l'UE assuma un ruolo di primo piano nel mercato globale della cybersicurezza.
2. **Affrontare le lacune dei cyberattacchi:** Rispondere ai limiti dei quadri esistenti, che hanno faticato ad affrontare efficacemente i recenti attacchi informatici.
3. **Opportunità geopolitica:** Rispondere al crescente dibattito sulla sicurezza dei sistemi informativi e delle reti, allineandosi alla strategia geopolitica dell'UE.

ENISA

Rafforzare il ruolo dell'ENISA

L'articolo 3 del mandato della legge sulla cibersicurezza delinea il ruolo dell'ENISA nel raggiungimento di un livello elevato di cibersicurezza in tutta l'UE:

1. **Supporto e competenze:** L'ENISA supporta gli Stati membri, le istituzioni dell'UE e le altre parti interessate, fungendo da punto di riferimento fondamentale per le consulenze e le competenze in materia di cibersicurezza.
2. **Ridurre la frammentazione del mercato:** L'ENISA contribuisce ad armonizzare le leggi e i regolamenti sulla cybersicurezza nei vari Stati membri per ridurre la frammentazione.
3. **Indipendenza e coordinamento:** L'ENISA opera in modo indipendente, garantendo di integrare, anziché duplicare, gli sforzi nazionali e di sfruttare le competenze esistenti negli Stati membri.
4. **Sviluppo delle risorse:** L'ENISA ha il compito di sviluppare le risorse tecniche e umane necessarie per adempiere ai suoi compiti di sicurezza informatica.

ENISA - Obiettivi

- Responsabilizzazione delle comunità
- Politica di sicurezza informatica
- Cooperazione operativa Sviluppo di capacità
- Soluzioni affidabili e lungimiranti
- Conoscenza

Schemi di certificazione

Sistemi di certificazione

Il considerando 69 del Cybersecurity Act sottolinea la necessità di un quadro europeo unificato di certificazione della cybersecurity. I punti chiave includono:

- **Approccio comune:** Stabilire un quadro europeo di certificazione per i prodotti, i servizi e i processi ICT da riconoscere in tutti gli Stati membri dell'UE.
- **Basarsi sui sistemi esistenti:** Sfruttare i sistemi di certificazione nazionali e internazionali esistenti, come il SOG-IS, per una transizione agevole al nuovo quadro.
- **Duplicare scopo:** il quadro mira a creare fiducia nei prodotti e nei servizi TIC certificati e a ridurre la proliferazione di schemi di certificazione nazionali in conflitto tra loro, riducendo i costi per le imprese nel mercato unico digitale.
- **Standard:** I sistemi di certificazione devono essere non discriminatori e basati su standard europei o internazionali, a meno che tali standard non siano inadeguati per raggiungere gli obiettivi dell'UE.

Schemi di certificazione - definizione

L'articolo 2 definisce:

- **Schema europeo di certificazione della sicurezza informatica:** Un insieme di regole, requisiti tecnici, standard e procedure a livello di Unione per la certificazione di prodotti, servizi o processi ICT.
- **Schema nazionale di certificazione della sicurezza informatica:** Un insieme di regole, requisiti tecnici, standard e procedure stabiliti da un'autorità nazionale per certificare prodotti, servizi o processi ICT nell'ambito di quello specifico schema nazionale.

Schemi di certificazione - procedura

Articolo 47

Prodotti, servizi o processi TIC specifici sono inclusi nel programma di lavoro modulato dell'Unione per la certificazione della cibersecurity sulla base di fattori quali l'esistenza di schemi di certificazione nazionali che potrebbero portare alla frammentazione, le leggi o le politiche nazionali o dell'UE pertinenti, la domanda di mercato, i cambiamenti nel panorama delle minacce informatiche e le richieste del Gruppo europeo di certificazione della cibersecurity (ECCG) per schemi specifici. Nella stesura del programma di lavoro, la Commissione europea tiene conto anche del feedback dell'ECCG e dello Stakeholder Certification Group.

Articolo 51

Gli schemi di certificazione europei di cybersecurity mirano a proteggere i dati da accessi, elaborazioni o divulgazioni non autorizzate durante tutto il loro ciclo di vita, salvaguardandoli da distruzione, perdita, alterazione o indisponibilità accidentali. Garantiscono che l'accesso ai dati o ai servizi sia limitato a persone o sistemi autorizzati, che le dipendenze e le vulnerabilità siano identificate e documentate e che l'accesso, l'utilizzo e l'elaborazione di dati, servizi o funzioni siano registrati e monitorati. Questi schemi consentono inoltre di verificare chi ha avuto accesso o elaborato dati, servizi o funzioni, assicurano che i prodotti, i servizi e i processi TIC siano privi di vulnerabilità note e supportano il recupero tempestivo di dati e servizi in caso di incidenti. Garantiscono inoltre che i prodotti, i servizi e i processi TIC siano sicuri per progettazione e per impostazione predefinita, mantenendo software e hardware aggiornati con meccanismi di aggiornamento sicuri per affrontare le vulnerabilità note.

Schemi di certificazione - governance

Articolo 58 - Autorità nazionali di certificazione della cibersecurity

Ogni Stato membro deve designare una o più autorità nazionali di certificazione della cybersecurity o, con l'accordo di un altro Stato membro, designare autorità di quel Paese. Queste autorità devono essere indipendenti in termini di organizzazione, finanziamento e decisioni.

Gli Stati membri hanno la responsabilità di garantire che queste autorità dispongano di risorse adeguate per svolgere efficacemente i loro compiti.

Articolo 97 - Domanda di certificazione e accreditamento

Una volta adottato uno schema europeo di certificazione della cybersecurity, i produttori o i fornitori di servizi possono presentare domande di certificazione a qualsiasi organismo di valutazione della conformità accreditato nell'UE. Questi organismi devono essere accreditati dagli enti di accreditamento nazionali, con accreditamento che dura fino a cinque anni ed è rinnovabile a determinate condizioni. Gli enti nazionali di accreditamento possono limitare o revocare l'accREDITAMENTO in caso di mancato rispetto dei requisiti o di violazione dei regolamenti.

Schemi di certificazione - valutazione della conformità

- Uno schema europeo di certificazione della cybersecurity può consentire ai produttori o ai fornitori di prodotti, servizi o processi ICT di eseguire un'autovalutazione della conformità. Ciò è consentito solo per prodotti o servizi a basso rischio, corrispondenti al livello di garanzia "base".
- I produttori o i fornitori possono rilasciare una dichiarazione di conformità UE, dichiarando che il loro prodotto, servizio o processo TIC soddisfa i requisiti dello schema. Così facendo, si assumono la responsabilità di garantire la conformità.
- Il produttore o il fornitore deve mettere a disposizione dell'autorità nazionale di certificazione della cybersecurity e dell'ENISA la dichiarazione di conformità UE, insieme alla documentazione tecnica e ad altre informazioni pertinenti, per un periodo di tempo determinato.
- Il rilascio della dichiarazione di conformità UE è volontario, a meno che non sia richiesto dalla legislazione
- dell'Unione o degli Stati membri. Le dichiarazioni di conformità UE sono riconosciute in tutti gli Stati membri.

Schemi di certificazione

1. **Sistema centralizzato:** In un di certificazione centralizzato, un'unica autorità centrale (come l'Unione Europea o un organismo nazionale) è responsabile della supervisione e della gestione del processo di certificazione. Questo organismo centrale stabilisce gli standard, approva la certificazione e rilascia le certificazioni. L'obiettivo è garantire l'uniformità e la coerenza del sistema.
2. **Sistema granulare:** Un sistema di certificazione granulare prevede più livelli o categorie di certificazione, ognuno dei quali si rivolge ad aree specifiche di prodotti, servizi o processi ICT. In questo sistema, le certificazioni possono variare a seconda di fattori quali il tipo di prodotto, il suo livello di rischio o la sua applicazione. Questo approccio consente valutazioni di conformità più personalizzate e dettagliate.
3. **Effetto legale:** L'effetto legale si riferisce alla natura vincolante della certificazione. In alcuni casi, le certificazioni possono avere conseguenze legali, nel senso che una volta che un prodotto, un servizio o un processo è certificato, viene considerato conforme a leggi o regolamenti specifici. Questo potrebbe impatto sull'accesso al mercato, sulla responsabilità o sugli obblighi di conformità.

Proposta di revisione della legge sulla cybersecurity

La proposta modifica il regolamento (UE) 2019/881 per includere i **servizi di sicurezza gestiti** come soggetti per la certificazione di cybersecurity.

schemi. I servizi di sicurezza gestiti comprendono attività come la gestione del rischio di cybersecurity, la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza.

L'articolo 51a delinea gli obiettivi di sicurezza per gli schemi di certificazione dei servizi di sicurezza gestiti, che comprendono:

1. Assicurarsi che i fornitori di servizi dispongano di personale altamente competente, con competenze tecniche, esperienza e integrità professionale.

2. Garantire che il fornitore mantenga procedure interne di alta qualità per l'erogazione dei servizi.
3. Proteggere i dati da accessi, archiviazione, divulgazione, distruzione o alterazione non autorizzati.
4. Garantire il ripristino tempestivo dell'accesso a dati, servizi e funzioni dopo gli incidenti.
5. Limitare l'accesso ai dati al solo personale autorizzato.
6. Registrazione e valutazione dell'utilizzo, dell'accesso e dell'elaborazione dei dati.
7. Garantire che i prodotti, i servizi e i processi TIC utilizzati siano sicuri di default, privi di vulnerabilità note e regolarmente aggiornati con le ultime patch di sicurezza.

Standardizzazione della sicurezza informatica

Gli standard sono documenti che definiscono specifiche, procedure e linee guida per garantire la sicurezza, la coerenza e l'affidabilità di prodotti, servizi e sistemi. Questi standard sono basati su accordi generali e convalidati da enti legali, che fungono da linee guida o modelli in contesti specifici (ad esempio, ISO/IEC).

Nel contesto della sicurezza informatica, gli standard si concentrano sulle caratteristiche di sicurezza delle applicazioni e degli algoritmi crittografici, enfatizzando i controlli di sicurezza, i processi, le procedure e le linee guida volte a prevenire o attenuare gli attacchi informatici e a ridurre i rischi di minaccia informatica.

I vantaggi degli standard includono:

- Risparmio di tempo, riduzione dei costi e aumento dei profitti
- Maggiore consapevolezza degli utenti e riduzione dei rischi
- Continuità aziendale e conformità alle migliori pratiche del settore Opportunità di confronto internazionale dei sistemi di sicurezza

Classificazione degli standard:

- Sicurezza delle informazioni (ad esempio, serie ISO 27000, NIST, SOX)
- Governance della sicurezza delle informazioni

Distinzione chiave:

- **Gli standard di cybersecurity** forniscono metodi e aspettative dettagliate per il completamento dei processi.
- **I framework di cybersecurity** sono linee guida più ampie che coprono vari componenti o domini senza specificare i passi esatti da seguire.

Famiglie di standard IS

1. **Serie ISO 27000:** Questa è la categoria centrale, da cui si diramano diversi standard ISO/IEC.
2. **BSI (British Standards Institution):** Include diversi standard BSI
3. **SoGP:** si riferisce a un altro gruppo di standard, probabilmente specifici per alcune linee guida operative (anche se questa parte è meno definita nell'immagine).
4. **Standard di settore:** Questa sezione comprende vari standard specifici del settore

Famiglie di quadri di IS

- **Serie NIST SP 800:** Questa è la categoria centrale, con diversi framework del NIST (National Institute of Standards and Technology).
- **COBIT:** un altro importante framework, COBIT (Control Objectives for Information and Related Technologies), è citato come riferimento chiave nel diagramma, spesso utilizzato per la governance e la gestione dell'IT.

Schema di certificazione dei criteri comuni dell'UE

Il primo schema di certificazione della sicurezza informatica

Regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024

che stabilisce le regole per l'applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema di certificazione della cibersicurezza basato sui criteri comuni europei (EUCC)

Contesto - Livello europeo

Il **SOG-IS MRA** (Senior Officials Group Information Systems Security Mutual Recognition Agreement), istituito in risposta alle decisioni del Consiglio dell'UE del 1992 e del 1995 e aggiornato nel 2010, mira a standardizzare la valutazione della sicurezza informatica in Europa. I suoi obiettivi principali

includono il coordinamento dei profili di protezione e delle politiche di certificazione dei Common Criteria (CC) tra gli organismi di certificazione europei per garantire l'allineamento con il gruppo internazionale CCRA, nonché lo sviluppo di profili di protezione in risposta alle direttive dell'UE in materia di sicurezza informatica.

I partecipanti all'MRA sono organizzazioni o agenzie governative dei paesi dell'UE e dell'EFTA, impegnate a garantire standard elevati e coerenti nella valutazione dei prodotti IT per aumentare la fiducia nella loro sicurezza, aumentando la disponibilità di prodotti valutati e sicuri. prodotti informatici migliorati, evitando duplicazioni di valutazioni e migliorando l'efficienza e l'economicità dei processi di valutazione e certificazione.

Nel giugno 2023, il Comitato di gestione MRA del SOG-IS ha approvato l'adozione della versione CC:2022 dei Common Criteria per l'emissione dei certificati.

Contesto - Livello internazionale

ISO/IEC 15408 (Common Criteria) è uno standard internazionale per la valutazione della sicurezza di prodotti e sistemi informatici, composto da tre parti principali:

1. **Parte 1** - Introduzione e modello generale: Fornisce una panoramica dei concetti di valutazione della sicurezza informatica e un modello generale di valutazione.
2. **Parte 2** - Requisiti funzionali di sicurezza: Definisce i componenti funzionali standard per esprimere i requisiti di sicurezza dei target di valutazione (TOE).
3. **Parte 3** - Requisiti di sicurezza: Stabilisce le componenti di sicurezza per valutare l'affidabilità dei TOE.

Lo standard include un catalogo di componenti che affrontano vari aspetti funzionali e di garanzia, sebbene sia troppo specializzato per scopi più ampi di tassonomia della cybersecurity.

Il **Common Criteria Recognition Arrangement (CCRA)** consente ai laboratori autorizzati di valutare i prodotti rispetto a specifici criteri di sicurezza. proprietà. I prodotti certificati ricevono una certificazione riconosciuta da tutti i firmatari del CCRA, basata sui risultati della valutazione e supportata da linee guida per l'applicazione dei criteri a tecnologie specifiche.

Schema di certificazione EUCC

Lo schema **EUCC (European Cybersecurity Certification)**, proposto per la prima volta il 1° luglio 2020, è un candidato alla certificazione di cybersecurity. destinato a sostituire gli schemi di Accordo di Mutuo Riconoscimento (ARR) SOG-IS. L'obiettivo è rafforzare il mercato interno e migliorare la sicurezza dei prodotti TIC, in particolare quelli con funzioni di sicurezza integrate (ad esempio, firewall, dispositivi di crittografia, router, smartphone, ecc.)

Caratteristiche principali dello schema EUCC:

- **Livelli di garanzia:** Offre due livelli di garanzia di sicurezza, "sostanziale" ed "elevato", adatti a prodotti con requisiti di sicurezza elevati. Non include un livello base, escludendo così le opzioni di autovalutazione.
- **Obiettivo:** Fornire ai consumatori una valutazione imparziale della sicurezza dei prodotti ICT, aumentando la fiducia nei prodotti certificati attraverso analisi dettagliate e test rispetto a specifici standard di sicurezza.

L'attuale schema **Common Criteria (CC)**, riconosciuto da 15 Paesi dell'UE e da oltre 30 altre nazioni, ha certificato più di 4.500 prodotti. All'interno dell'UE, specifici schemi nazionali operano secondo i principi dei Common Criteria, gestiti da agenzie come ANSSI (Francia), BSI (Germania) e OCSI (Italia). Questi schemi seguono criteri di valutazione, requisiti di sicurezza e livelli di garanzia simili.

La proposta stabilisce le norme per l'attuazione del **Regolamento (UE) 2019/881** relativo all'adozione del **sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)**. Questo sistema, basato sugli standard Common Criteria, stabilisce i requisiti e le linee guida per certificare la sicurezza dei prodotti ICT all'interno dell'UE, con l'obiettivo di armonizzare gli standard di cybersecurity tra gli Stati membri e aumentare la fiducia nei prodotti certificati.

Schema di certificazione EUCC

Per ottenere un certificato EUCC, il richiedente deve fornire la documentazione sull'uso previsto del prodotto ICT e un'analisi di livelli di rischio associati. Ciò consente all'organismo di valutazione della conformità di verificare che il livello di garanzia scelto sia appropriato. Se lo stesso organismo gestisce sia la valutazione che la certificazione, il richiedente deve presentare queste informazioni una sola volta.

Un **dominio tecnico** è un quadro di riferimento per i prodotti ICT con funzioni di sicurezza specifiche e simili che affrontano tipi comuni di attacchi, favorendo valutazioni coerenti.

I due principali domini tecnici attualmente utilizzati per la certificazione sono:

- **AVA_VAN.4:** Per "smart card e dispositivi simili", dove la sicurezza si basa su elementi hardware personalizzati (ad esempio, hardware di smart card, Trusted Platform Modules).
- **AVA_VAN.5:** per i "dispositivi hardware con box di sicurezza", utilizzo di un involucro fisico protettivo ("Security Box") per resistere agli attacchi diretti (ad esempio, terminali di pagamento, tachigrafi e moduli di sicurezza hardware).

Conflitto tra sicurezza e privacy

Valori protetti dalla cybersecurity

Identificazione e implementazione di misure e tecniche per la protezione delle informazioni da: accesso, uso, modifica, distruzione, divulgazione o interruzione non autorizzati.

Valori protetti: sicurezza, privacy, equità, responsabilità

Sicurezza

La sicurezza è lo stato di assenza di pericolo o minaccia. Comprende la protezione contro un danno intenzionale, distinguendosi da sicurezza, che si riferisce alla protezione da pericoli accidentali o non intenzionali. La sicurezza è caratterizzata dall'assenza di pericolo o minaccia.

La privacy

La privacy informativa riguarda le informazioni su un individuo che sono (o non sono) note o condivise con altri. Si tratta di una distinzione tra riservatezza o segretezza dei dati e controllo su quali dati vengono condivisi con chi.

Equità

Le minacce e le misure di cybersecurity hanno impatto diverso sulle persone, sollevando questioni di uguaglianza, giustizia, non discriminazione e democrazia. L'equità nella cybersecurity riguarda la necessità di un trattamento e di risultati equi per tutti gli individui.

Responsabilità

La responsabilità riguarda la trasparenza, l'apertura e la spiegabilità. Si tratta di due scenari: uno in cui qualcuno danneggia un altro o ne viola i diritti, e un altro in cui esiste uno squilibrio di potere, in cui l'agente più potente può introdurre regole o misure che possono danneggiare i meno potenti.

Privacy contro sicurezza

La sicurezza si ottiene a costo della privacy. La sicurezza aiuta a raggiungere la privacy. La privacy richiede un certo grado di sicurezza informatica. La privacy è ottenuta al costo della sicurezza. La privacy contribuisce alla sicurezza.

GDPR - Protezione dei dati

Fonti legali

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, GU L 119 del 04.05.2016.

Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) Decreto legislativo 10

- agosto 2018, n. 101

Dati personali - definizione

I dati personali sono definiti come informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, ecc.

- Dati che consentono l'identificazione diretta e dati che consentono l'identificazione
- indiretta Dati sensibili e dati giudiziari
- Nuovi dati?
 - o Dati relativi alle comunicazioni elettroniche, dati di geolocalizzazione

Attori - definizioni

L'**interessato** è la persona fisica a cui si riferiscono i dati personali (articolo 4, paragrafo 1, punto 1 del GDPR).

Il **Titolare del trattamento** è la persona fisica, l'autorità pubblica, la società, l'ente pubblico o privato, l'associazione, ecc. che prende le decisioni sulle finalità e sui mezzi del trattamento (articolo 4, paragrafo 1, punto 7 del GDPR).

Il **responsabile del trattamento** è la persona fisica o giuridica a cui il titolare del trattamento chiede di svolgere per suo conto compiti specifici e definiti di gestione e controllo del trattamento dei dati (articolo 4, paragrafo 1, punto 8 del GDPR).

Ambito di applicazione del GDPR

Il Regolamento (UE) 2016/679 disciplina il trattamento dei dati personali indipendentemente dal fatto che sia effettuato o meno nell'UE:

- se effettuati da responsabili o incaricati del trattamento stabiliti nell'UE o in un luogo soggetto alla legge di uno Stato membro dell'UE in virtù del diritto pubblico internazionale

- oppure quando il responsabile del trattamento o l'incaricato del trattamento non è stabilito nell'Unione europea ma le attività di trattamento riguardano
 - l'offerta di beni o la fornitura di servizi ai suddetti interessati nell' Europa, indipendentemente dal fatto che il pagamento da parte dell'interessato sia obbligatorio
 - il monitoraggio del loro comportamento nella misura in cui questo avviene all'interno dell'Unione Europea

Diritti dell'interessato

L'interessato ha il diritto di chiedere al titolare del trattamento se i suoi dati personali sono stati trattati. Se i dati sono stati trattati, ha il diritto di ottenerne una copia e di essere informato sulle finalità del trattamento, sulle categorie di dati personali coinvolti, sui destinatari dei dati, sul periodo di conservazione dei dati, sulla loro origine, sugli estremi identificativi di coloro che trattano i dati, sulle modalità di trattamento dei dati.

L'esistenza di processi decisionali automatizzati (compresa la profilazione) e i diritti previsti dal Regolamento.

L'interessato può inoltre chiedere la rettifica dei propri dati personali, se inesatti o incompleti, la loro cancellazione, la limitazione del trattamento o il trasferimento a un altro titolare del trattamento, a condizione che il trattamento sia basato sul consenso o su un contratto stipulato con l'interessato e sia effettuato con mezzi automatizzati.

Inoltre, l'interessato ha il diritto di opporsi al trattamento dei propri dati personali per motivi legati alla sua situazione particolare.

situazione, specificando i motivi nella richiesta. Possono inoltre opporsi al trattamento dei loro dati per finalità di marketing diretto senza dover fornire alcuna motivazione.

Diritto all'oblio

Diritto alla cancellazione dei propri dati personali in forma estesa:

Obbligo per i responsabili del trattamento (se hanno "reso pubblici" i dati personali dell'interessato) di informare gli altri responsabili del trattamento dei dati personali cancellati della richiesta di cancellazione, compresi "qualsiasi link, copia o riproduzione" (articolo 17, paragrafo 2).

Elaborazione dei dati

Qualsiasi trattamento dei dati personali deve essere conforme ai seguenti principi

- Liceità, correttezza e trasparenza del trattamento, con riferimento 'interessato
- limitazione delle finalità del trattamento, compreso l'obbligo di garantire che qualsiasi ulteriore trattamento non sia incompatibile con le finalità della raccolta dati
- minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità del trattamento accuratezza e
- aggiornamento dei dati, compresa la tempestiva cancellazione dei dati inesatti in relazione alle finalità del trattamento limitazione della conservazione: i
- dati devono essere conservati per un periodo non superiore a quello necessario per le finalità per le quali sono trattati
- integrità e riservatezza: è necessario garantire un'adeguata sicurezza dei dati personali oggetto di trattamento

Trattamento legittimo dei dati - base giuridica

Il trattamento legittimo dei dati richiede una base giuridica valida, che può includere il consenso dell'interessato, l'adempimento di obblighi contrattuali o l'obbligo di fornire informazioni.

obblighi, protezione di interessi vitali dell'interessato o di , adempimento di obblighi legali a cui è soggetto il titolare del trattamento, trattamento per l'interesse pubblico o per l'esercizio di pubblici poteri e interessi legittimi prevalenti del titolare del trattamento o di terzi a cui vengono comunicati i dati. Per quanto riguarda le categorie speciali di dati personali, il trattamento è generalmente vietato, tranne che in condizioni specifiche.

Consenso

Per la validità del consenso è necessario che l'interessato sia stato informato del trattamento dei suoi dati personali, ai sensi degli articoli 13 o 14 del Regolamento. Il consenso deve essere espresso dall'interessato in modo libero, inequivocabile e specifico per ciascuna finalità del trattamento, se si tratta di più finalità. La richiesta di consenso deve essere distinta da altre richieste rivolte all'interessato. Inoltre, non è necessario che il consenso sia "documentato per iscritto", né è richiesta una "forma scritta".

Informazioni sul trattamento dei dati

Deve essere fornita all'interessato prima del trattamento, prima che i dati siano raccolti Il contenuto è

previsto dagli articoli 13, paragrafo 1, e 14, paragrafo 1

- identità del titolare del trattamento
- finalità del trattamento
- diritti dell'interessato dati di
- contatto del DPO

- interesse legittimo
- eventuale trasferimento a paesi terzi periodo
- di conservazione dei dati
- diritto di presentare un reclamo all'autorità di controllo eventuale
- processo decisionale automatizzato

In linea di principio, le informazioni vengono fornite per iscritto e preferibilmente in formato elettronico.

Deve essere comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice.

Trasferimento dei dati a paesi terzi

Il trasferimento dei dati personali verso paesi al di fuori dell'Unione Europea è vietato, tranne nei seguenti casi: adeguatezza al paese

- terzo riconosciuta da una decisione della Commissione Europea
- in assenza di una decisione di adeguatezza da parte della Commissione, adeguate garanzie contrattuali o di contratto
- in assenza di qualsiasi altro prerequisito, l'utilizzo di eccezioni al divieto di trasferimento applicabili in situazioni specifiche

Protezione dei dati Autorità di controllo

Il Gruppo di lavoro Articolo 29 è diventato il Consiglio europeo delle autorità di vigilanza (EDPB)

Autorità di vigilanza nazionali

- Il Garante per la protezione dei dati personali

Meccanismo dello sportello unico

I compiti e i poteri Autorità di vigilanza

Monitoraggio e supervisione, funzioni consultive, poteri investigativi, gestione dei reclami, poteri correttivi

Reclami in di violazione

Reclamo all'autorità di vigilanza

- l'istruttoria e l'eventuale procedura amministrativa formale che può portare all'adozione di rimedi e sanzioni amministrative

La decisione dell'autorità di vigilanza può essere impugnata in tribunale

Sanzioni amministrative ai sensi del GDPR (art. 83)

Sanzioni amministrative comminate dal DPA

principi delle sanzioni amministrative **Due gruppi di**

ammende ai sensi del GDPR:

- fino a 10 milioni di euro o il 2% del fatturato globale annuo se
- superiore fino a 20 milioni di euro o il 4% del fatturato globale annuo se superiore

Il principio di responsabilità nel campo della protezione dei dati

Il principio di responsabilità richiede che sia il titolare del trattamento che gli incaricati del trattamento garantiscano che il trattamento dei dati personali sia conforme alle norme pertinenti e siano in grado di dimostrare tale conformità in qualsiasi momento. È incentrato principalmente sul titolare del trattamento e adotta un approccio basato sul rischio, il che significa che il livello di conformità e le garanzie devono riflettere i rischi associati alle attività di trattamento. Gli "elementi" di responsabilità riguardano azioni come la documentazione, le politiche interne e le misure per garantire l'aderenza alle normative sulla protezione dei dati.

Il principio di responsabilità ai sensi del GDPR

Adozione di **codici di condotta, meccanismi di certificazione, sigilli e marchi di protezione dei dati** come strumenti di facilitazione per dimostrare l'adempimento degli obblighi del responsabile del trattamento (art. 24 par. 3 GDPR) e dell'incaricato del trattamento (art. 28 par. 5 GDPR), nonché fattori attenuanti di

sanzioni amministrative (Art 83 par 2 GDPR) Registro delle

attività di trattamento (Art 30 GDPR)

Misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR) Notifica di una violazione dei

dati personali al DPA (art. 33 GDPR)

Dalla RESPONSABILITÀ alla RESPONSABILITÀ

Articolo 82 GDPR (Diritto al risarcimento e responsabilità)

1. Chiunque abbia subito un danno materiale o morale a causa di una violazione del presente regolamento **ha il diritto di ottenere dal responsabile del trattamento o dall'incaricato del trattamento il risarcimento del danno subito.**
2. Il responsabile del trattamento coinvolto nel trattamento è responsabile dei danni causati dal trattamento che viola il presente regolamento.
L'incaricato del trattamento è responsabile dei danni causati dal trattamento solo se non ha rispettato gli obblighi del presente regolamento specificamente diretti agli incaricati del trattamento o se ha agito al di fuori o contro le istruzioni legittime del responsabile del trattamento.
3. **Il responsabile del trattamento o l'incaricato del trattamento è esonerato dalla responsabilità di cui al paragrafo 2 se dimostra di non essere in alcun modo responsabile dell'evento che ha provocato il danno**

GDPR - Valutazione del rischio e violazione dei dati

Il rischio nel GDPR

Art. 24 GDPR Misure tecniche e organizzative 24 GDPR Misure tecniche e organizzative

Tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire e poter dimostrare che il trattamento è effettuato in conformità al presente regolamento.

Tali misure saranno riesaminate e aggiornate se necessario. 25 protezione dei dati per disegno e per difetto

Tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche posti dal trattamento, il titolare del trattamento, sia al momento della determinazione dei mezzi per il trattamento che al momento del trattamento stesso, mette in atto misure tecniche e organizzative adeguate, come la pseudonimizzazione, che mirano a

Art. 32 GDPR Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento attuano misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio, tra l'altro in modo appropriato:
 - a. la pseudonimizzazione e la crittografia dei dati personali;
 - b. la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione;
 - c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
 - d. un processo di verifica, valutazione e verifica periodica dell'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza si terrà conto in particolare dei rischi che il trattamento comporta, in particolare la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati.

Art 35 DPIA

Se un tipo di trattamento, in particolare quello che utilizza nuove tecnologie, e tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento deve, prima del trattamento, una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali. Un'unica valutazione può riguardare un insieme di trattamenti simili che presentano rischi elevati simili.

Che cos'è un rischio?

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimate in termini di gravità e probabilità.

Catalogo dei rischi

Recital 75

Il rischio per i diritti e le libertà delle persone fisiche, di varia probabilità e gravità, può derivare dal trattamento dei dati personali che potrebbe portare a danni fisici, materiali o immateriali, in particolare:

- quando il trattamento può dar luogo a discriminazioni, furti di identità o frodi, perdite finanziarie, danni alla reputazione, perdita di riservatezza di dati personali protetti da segreto professionale, inversione non autorizzata della pseudonimizzazione o qualsiasi altro svantaggio economico o sociale significativo;
- quando gli interessati potrebbero essere privati dei loro diritti e libertà o impossibilitati a esercitare il controllo sui loro dati personali; quando vengono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale e il trattamento di dati genetici, di dati relativi alla salute o di dati relativi alla vita sessuale o alle condanne penali e ai reati o alle relative misure di sicurezza;
- in cui vengono valutati gli aspetti personali, in particolare analizzando o prevedendo gli aspetti relativi al rendimento sul lavoro, all'aspetto economico situazione, salute, preferenze o interessi personali, affidabilità o comportamento, ubicazione o spostamenti, al fine di creare o utilizzare profili personali; in caso di trattamento di dati personali di persone fisiche vulnerabili, in particolare di bambini;
- o quando il trattamento coinvolge una grande quantità di dati personali e riguarda un gran numero di interessati.

DPIA

Gli effetti complessivi del trattamento dei dati possono includere danni alla reputazione, discriminazioni, furti d'identità, perdite finanziarie, danni fisici o di immagine. danni psicologici, perdita di controllo sui dati personali e altri svantaggi economici o sociali. Inoltre, le persone possono trovarsi nell'impossibilità di esercitare i propri diritti, accedere ai servizi o sfruttare le opportunità a causa di un trattamento improprio dei loro dati.

Valutazione del rischio

"La valutazione del rischio" può essere definita come l'insieme delle attività coordinate per dirigere e controllare un'organizzazione in relazione al rischio.

Elementi da considerare nella valutazione del rischio: origine, natura, gravità, **probabilità**, **impatto** sui diritti e sulle libertà delle persone Considerando 76

La probabilità e la gravità dei rischi per i diritti e le libertà degli individui devono essere determinate con riferimento : • La natura

- Ambito di applicazione
- Contesto
- Finalità del trattamento

Livello di impatto	Descrizione
Basso	Gli individui possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per inserire nuovamente le informazioni, fastidi, irritazioni, ecc.)
Medio	Gli individui possono incontrare disagi significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione dell'accesso ai servizi aziendali, paura, mancanza di comprensione, stress, piccoli disturbi fisici, ecc.)
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare, anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento delle condizioni di salute, ecc.)
Molto alto	Individui che possono andare incontro a conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, problemi psicologici o fisici a lungo termine). malattie, morte, ecc.)

DPIA

In linea con l'approccio basato sul rischio, l'esecuzione di una DPIA non è obbligatoria per ogni operazione di trattamento.

- La DPIA è richiesta solo quando un tipo di trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1).
- Il semplice fatto che non siano state soddisfatte le condizioni che fanno scattare l'obbligo di effettuare la DPIA non diminuisce, tuttavia, l'obbligo generale dei controllori di attuare misure per gestire in modo appropriato i rischi per la salute dei consumatori. diritti e libertà degli interessati.

In pratica, ciò significa che i responsabili del trattamento devono valutare costantemente i rischi creati dalle loro attività di trattamento per identificare quando un tipo di trattamento è "suscettibile di comportare un rischio elevato per i diritti e le libertà delle persone fisiche".

Che cos'è una DPIA?

Il GDPR non definisce formalmente il concetto di DPIA in quanto tale, ma il suo contenuto minimo è specificato dall'articolo 35(7):

- "a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compresa, se del caso, la legittima interesse perseguito dal responsabile del trattamento;
- (b) una valutazione della necessità e della proporzionalità del trattamento in relazione alle finalità;
- (c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- (d) le misure previste per affrontare i rischi, comprese le salvaguardie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenendo conto dei diritti e degli interessi legittimi dei dati soggetti e altre persone interessate”;

Quali trattamenti sono soggetti a una DPIA?

A parte le eccezioni, quando sono "suscettibili di comportare un rischio elevato".

Nei casi in cui non è chiaro se sia necessaria una DPIA, il WP29 raccomanda comunque di effettuarla, in quanto è uno strumento utile per aiutare i responsabili del trattamento a rispettare la normativa sulla protezione dei dati.

Anche se una DPIA potrebbe essere richiesta in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi quando un trattamento "può comportare rischi elevati":

- "a) una valutazione sistematica ed estesa degli aspetti personali relativi alle persone fisiche che si basa su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che producono effetti giuridici sulla persona fisica o che incidono in modo analogo e significativo sulla persona fisica¹²”;
- (b) trattamento su larga scala di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e reati di cui all'articolo 10; oppure
- (c) un monitoraggio sistematico di un'area accessibile al pubblico larga scala”.

Quando non è necessaria una DPIA?

Il WP29 ritiene che la DPIA non sia necessaria nei seguenti casi:

- quando il trattamento non è "suscettibile di comportare un rischio elevato per i diritti e le libertà delle persone fisiche".
- quando la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili al trattamento per il quale è stata la DPIA. In questi casi, possono essere utilizzati i risultati della DPIA per un trattamento simile;
- quando i trattamenti sono stati verificati da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- se un , ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), ha una base giuridica nel diritto dell'UE o degli Stati membri, se la legge disciplina il trattamento specifico e se è già stata effettuata una DPIA come parte della definizione di tale base giuridica;
- se il trattamento è incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) dei trattamenti per i quali non è richiesta la DPIA;

Come si effettua una DPIA? In quale momento deve essere effettuata una DPIA?

La DPIA deve essere effettuata "prima del trattamento". Ciò è coerente con i principi della protezione dei dati per progettazione e per impostazione predefinita. La DPIA deve essere vista come uno strumento per aiutare il processo decisionale relativo al trattamento.

La DPIA dovrebbe essere avviata il prima possibile nella fase di progettazione del trattamento, anche se alcune operazioni di trattamento sono ancora sconosciute. L'aggiornamento della DPIA durante l'intero ciclo di vita del progetto garantirà che la protezione dei dati e la privacy siano prese in considerazione e incoraggerà la creazione di soluzioni che promuovano la conformità.

L'esecuzione una DPIA è un processo continuo, non un esercizio una tantum.

Chi è obbligato a svolgere la DPIA?

Il responsabile del trattamento ha la responsabilità di garantire che la DPIA venga effettuata

L'esecuzione della DPIA può essere affidata a qualcun altro, all'interno o all'esterno dell'organizzazione, ma il responsabile del trattamento rimane in ultima analisi responsabile di tale compito.

Il responsabile del trattamento deve inoltre chiedere il parere del responsabile della protezione dei dati (DPO).

Se il trattamento è eseguito in tutto o in parte da un incaricato del trattamento, quest'ultimo deve assistere il responsabile del trattamento nell'esecuzione della DPIA e fornire tutte le informazioni necessarie.

Il responsabile del trattamento deve "chiedere il parere degli interessati o dei loro rappresentanti" "ove opportuno".

Sanzioni

L'inosservanza dei requisiti della DPIA può comportare multe da parte dell'autorità di vigilanza competente.

- Mancata esecuzione di una DPIA quando il trattamento è soggetto a una DPIA (articolo 35, paragrafi 1 e 3-4),
- esecuzione di una DPIA in modo scorretto (articolo 35, paragrafi 2 e 7-9),
- Non aver consultato l'autorità di vigilanza competente quando richiesto (articolo 36, paragrafo 3, lettera e)),

... può comportare una sanzione amministrativa pecuniaria fino a 10 milioni di euro o, nel caso di un'impresa, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Sicurezza e violazione dei dati

Il rischio nel GDPR

Art. 32 GDPR Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento attuano misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio, tra l'altro in modo appropriato:
 - a. la pseudonimizzazione e la crittografia dei dati personali;
 - b. la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione;
 - c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
 - d. un processo di verifica, valutazione e verifica periodica dell'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza si terrà conto in particolare dei rischi che il trattamento comporta, in particolare la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati.

Violazione dei dati personali

art. 4(12) : una violazione della sicurezza che comporti la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o altrimenti trattati. 4(12) : una violazione della sicurezza che comporti la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati.

- Non tutte le violazioni sono violazioni di dati
 - Una violazione della sicurezza se non vi è alcuna prova che abbia portato a "distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali trasmessi, memorizzati o altrimenti trattati".
- Trattamento illecito di dati personali non dovuto a un incidente di sicurezza.

Quadro di gestione delle violazioni dei dati

Recital 87

Occorre verificare se sono state messe in atto tutte le misure tecnologiche di protezione e organizzative adeguate per stabilire immediatamente se si è verificata una violazione dei dati personali e per informare tempestivamente l'autorità di controllo. autorità e l'interessato Prevenire

1. Educare
2. Ridurre al minimo (raccolta dati, accesso ai dati, archivi di dati, ...)
3. Smaltire in modo sicuro
4. Proteggere i dispositivi mobili (crittografia, aggiornamenti e patch, ...)
5. Reti sicure (VPN)
6. Mantenere il software e l'hardware aggiornati e mantenuti
7. Gestire gli appaltatori

8. Sviluppare e comunicare chiaramente le politiche
9. Prepararsi al peggio (risposta all'incidenza, recupero in caso di disastro)

10. Rileva

mento

dell'audit

Per identificare un incidente di sicurezza, è essenziale determinare cosa è successo, quando si è verificato, chi è stato coinvolto e dove è verificato. A

Un problema significativo è il gap di rilevamento delle violazioni, poiché circa il 90% delle compromissioni avviene entro secondi o minuti, ma il rilevamento entro secondi o ore rappresenta solo il 25% circa delle violazioni (ETL 2016). Gli strumenti per il rilevamento comprendono la registrazione e il monitoraggio, nonché il rilevamento delle intrusioni e gli avvisi.

La comprensione della causa principale implica la determinazione dell'origine della violazione. È stata causata da un firewall con una porta aperta, da un malware nel sistema, da un attacco di phishing via e-mail, da un software antivirus obsoleto o da un dipendente che ha accidentalmente divulgato dati personali? Gli strumenti per questa fase includono l'analisi forense e gli audit.

Una volta identificata la violazione e compresa la sua causa, l'incidente deve essere escalation e segnalato internamente ai team competenti per ulteriori azioni.

Valutare

- Per determinare se si tratta di una violazione di dati personali, occorre valutare se vi sono stati accessi non autorizzati, divulgazione o perdita di dati personali che potrebbero danneggiare gli interessati.
- Verificare le misure tecniche e organizzative esaminando le politiche di sicurezza, gli audit e i controlli come la crittografia e le restrizioni di accesso.
- Notificare a un'autorità competente se la violazione mette a rischio i diritti delle persone, entro 72 ore dalla scoperta.
- Notificare alle persone interessate se la violazione presenta un rischio elevato per i loro diritti, tenendo conto di fattori quali il tipo di dati, il numero di persone interessate e il tempo trascorso tra la violazione e la rilevazione.

Mitigare

Adottare misure immediate isolando il sistema interessato, cambiando le password e rimuovendo le pagine web compromesse, se possibile. Assicurarsi che i sistemi non siano più a rischio risolvendo il problema. Documentate tutte le azioni intraprese e implementate misure correttive per prevenire future violazioni. Infine, informare le parti interessate sia internamente che esternamente.

Comunicare (1)

Dal processore al controllore (interno)

- Art. 33 (2) GDPR: l'incaricato del trattamento deve notificare il responsabile del trattamento immediatamente dopo essere venuto a conoscenza della violazione dei dati.
- Art. 28(3)(f) GDPR: gli incaricati del trattamento devono anche assistere i responsabili del trattamento nel garantire l'osservanza dell'obbligo di questi ultimi di notificare una violazione al DPA.

Comunicare (2) Dal

controllore al DPA

- Art. 33(1) GDPR : In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione dei dati personali all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza...
- a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. [...].
- Art. 33 (4) GDPR: se e nella misura in cui non è possibile fornire le informazioni contemporaneamente, le informazioni possono essere fornite in fasi successive senza indebito ritardo.

Comunicare (3)

Notifica alla DPA

- Natura della violazione, categorie e numero approssimativo di soggetti interessati, categorie e numero approssimativo di record di dati personali interessati.
- Nome e informazioni di contatto del DPO o di un altro punto di contatto.
- Probabili conseguenze violazione.
- Descrizione delle misure adottate o che si propone di adottare per affrontare la violazione, nonché delle misure per mitigare i possibili effetti negativi della violazione.
- Informazioni aggiuntive

Comunicare (4)
agli interessati

Ai sensi dell'art. 33(3) del GDPR, se una violazione può comportare un rischio elevato per i diritti e le libertà delle persone, il titolare del trattamento deve notificarlo all'interessato senza indebito ritardo. Tuttavia, esistono delle eccezioni:

- Se il titolare del trattamento ha attuato misure tecniche e organizzative adeguate, come la crittografia, che sono state applicate prima della violazione, rendendo i dati personali incomprensibili a persone non autorizzate.
- Se sono state adottate misure successive per garantire che il rischio elevato per gli interessati non si verifichi più.
- Se la notifica agli interessati comporta uno sforzo sproporzionato, in tal caso si può ricorrere comunicazione pubblica.

Comunicare (5) agli interessati

Informazioni da fornire alle persone

- Nome e informazioni di contatto del DPO o di un altro punto di contatto.
- una descrizione delle probabili conseguenze della violazione dei dati personali; e
- una descrizione delle misure adottate, o che si propone di adottare, per far fronte alla violazione dei dati personali, comprese, se del caso, le misure adottate per attenuare eventuali effetti negativi.

Comunicare (5) al pubblico

Non vi è alcun obbligo legale di comunicare con il pubblico in generale, a meno che la violazione non comporti un rischio elevato per i diritti e le libertà delle persone e la notifica diretta agli interessati sarebbe sproporzionata. In questi si può alla comunicazione pubblica.

La trasparenza delle violazioni dei dati svolge un ruolo fondamentale nel creare fiducia tra gli interessati e i responsabili del trattamento. È anche un aspetto importante del patrimonio di un'organizzazione, in quanto un solido quadro di conformità può accrescere il valore dell'azienda, in particolare in scenari come fusioni o acquisizioni. Inoltre, la trasparenza aiuta a proteggere la reputazione dell'organizzazione dimostrando responsabilità nel trattamento dei dati personali.

Strategia europea per i dati

Comunicazione, Una strategia europea per i dati, 19.2.2020, COM(2020) 66 definitivo.

"Lo spazio europeo dei dati darà alle imprese dell'UE la possibilità di sfruttare le dimensioni del mercato unico. Norme europee comuni e meccanismi di applicazione efficienti dovrebbero garantire che:

- I dati possono fluire all'interno dell'UE e tra i vari settori;
- Le norme e i valori europei, in particolare la protezione dei dati personali, la legislazione sulla tutela dei consumatori e il diritto della concorrenza, sono pienamente rispettati;
- le regole per l'accesso e l'uso dei dati sono eque, pratiche e chiare, e ci sono meccanismi di governance dati chiari e affidabili; c'è un approccio aperto ma assertivo ai flussi internazionali di dati, basato sui valori europei."

Sfide per l'economia dei dati

Il valore dei dati deriva dal loro utilizzo e riutilizzo, a sostegno del bene pubblico attraverso varie interazioni come G2B, B2B, B2G e G2G. Gli squilibri del potere di mercato possono verificarsi quando i dati sono controllati da poche entità.

L'interoperabilità, la qualità, la struttura e l'integrità dei dati sono fondamentali per massimizzarne il valore, soprattutto con l'IA. Un'adeguata governance dei dati, supportata dalle giuste infrastrutture e tecnologie, garantisce una gestione efficace. La responsabilizzazione delle persone nell'esercizio dei loro diritti è fondamentale per il controllo e la protezione dei dati.

Legge sui dati

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alle norme armonizzate sull'accesso e l'uso corretto dei dati (Data Act) Articolo 1

Oggetto e ambito di applicazione

- Il presente regolamento stabilisce norme armonizzate sulla messa a disposizione dei dati relativi a prodotti e servizi agli utenti di prodotti connessi o servizi correlati, sulla messa a disposizione dei dati da parte dei titolari dei dati ai destinatari e sulla fornitura dei dati da parte dei titolari dei dati al pubblico. organismi del settore, la Commissione europea, la Banca centrale europea e gli organismi dell'Unione, se necessario per compiti di pubblico. Inoltre, il regolamento prevede la facilitazione del passaggio da un servizio di elaborazione dati all'altro, la salvaguardia dall'accesso illecito di terzi ai dati non e lo sviluppo di standard di interoperabilità per l'accesso, il trasferimento e l'utilizzo dei dati.
- Il presente regolamento si applica ai fabbricanti di prodotti connessi e ai fornitori di servizi connessi nell'Unione, indipendentemente dalla loro ubicazione, agli utenti di prodotti connessi o di servizi connessi nell'Unione e ai titolari dei dati che mettono i dati a disposizione dei destinatari nell'Unione, indipendentemente dalla loro ubicazione. Si applica inoltre ai destinatari dei dati nell'Unione, agli enti del settore pubblico, alla Commissione europea, alla Banca centrale europea e agli enti dell'Unione che richiedono dati per compiti di interesse pubblico, nonché ai titolari dei dati che forniscono tali dati. Inoltre, comprende i fornitori di servizi di elaborazione dati ai clienti nell'Unione, indipendentemente dalla loro ubicazione, e i partecipanti

negli spazi dati, i venditori di applicazioni che utilizzano i contratti intelligenti e gli individui coinvolti nell'implementazione di contratti intelligenti per altri nell'esecuzione di accordi.

Attori

- (11) Per "interessato" si intende l'interessato di cui all'articolo 4, punto (1), del Regolamento (UE) 2016/679;
- (12) Per "utente" si intende una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti per contratto i diritti temporanei di utilizzo di tale prodotto connesso, o che riceve servizi connessi;
- (13) Per "titolare dei dati" si intende una persona fisica o giuridica che ha il diritto o l'obbligo, ai sensi del presente regolamento, del diritto dell'Unione applicabile o della legislazione nazionale adottata in conformità al diritto dell'Unione, di utilizzare e rendere disponibili i dati, anche se concordato contrattualmente, dati relativi al prodotto o ai servizi correlati che ha recuperato o generato durante la fornitura di un servizio correlato;
- (14) Per "destinatario dei dati" si intende una fisica o giuridica che agisce per scopi connessi con l'attività commerciale, imprenditoriale, artigianale o con la sua attività professionale, diversi dall'utente di un prodotto connesso o di un servizio correlato, ai quali il titolare dei dati mette a disposizione i dati, compresi i terzi a seguito di una richiesta dell'utente al titolare dei dati o in conformità a un obbligo legale ai sensi del diritto dell'Unione o della legislazione nazionale adottata in conformità al diritto dell'Unione

Data Act: Scambio di dati B2G

Capitolo V - Messa a disposizione dei dati agli enti pubblici, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione sulla base di una necessità eccezionale

Articolo 14 - Obbligo di rendere disponibili i dati sulla base di una necessità eccezionale

Qualora un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione dimostri **la necessità eccezionale**, di cui all'articolo 15, di utilizzare determinati dati, compresi i metadati pertinenti necessari per interpretare e utilizzare tali dati, per svolgere i propri compiti di legge nel pubblico interesse, i titolari dei dati che sono persone giuridiche, diverse dagli enti pubblici, che detengono tali dati li mettono a disposizione su richiesta debitamente motivata.

Legge sui dati e sicurezza informatica

Articolo 15 - Necessità eccezionale di utilizzare i dati

1. La necessità eccezionale di utilizzare determinati dati ai sensi del presente capitolo è limitata nel tempo e nella portata e si considera sussistente solo in una delle seguenti circostanze:
 - (a) quando i dati richiesti sono necessari per rispondere a un'emergenza pubblica e l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione non sono in grado di ottenere tali dati con mezzi alternativi in modo tempestivo ed efficace in condizioni equivalenti;
 - (b) in circostanze non contemplate dalla lettera a) e solo per quanto riguarda i dati non personali, quando:
 - un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione agisce sulla base del diritto dell'Unione o nazionale e ha individuato dati specifici la cui mancanza gli impedisce di adempiere a un compito specifico svolto nel pubblico interesse, che sia stato esplicitamente previsto dalla legge, come la produzione di statistiche ufficiali o l'attenuazione o il recupero di un'emergenza pubblica; e
 - l'ente pubblico, la Commissione, la Banca centrale europea o l'ente dell'Unione ha esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati, compreso l'acquisto di dati non personali sul mercato offrendo tariffe di mercato, o facendo affidamento sugli obblighi esistenti di rendere disponibili i dati o sull'adozione di nuove misure legislative che potrebbero garantire la tempestività dei dati.

Scambio di dati B2G

(29) "emergenza pubblica": una situazione eccezionale, limitata nel tempo, come un'emergenza sanitaria, un'emergenza derivante da calamità naturali, una grave catastrofe provocata dall'uomo, **compreso un grave incidente di cibersicurezza**, che colpisce negativamente la popolazione dell'Unione o l'intero territorio di uno Stato membro o parte di esso, con un rischio di ripercussioni gravi e durature sulle condizioni di vita o sulla stabilità economica, sulla stabilità finanziaria o sul degrado sostanziale e immediato dei beni economici nell'Unione o nello Stato membro interessato e che è determinata o dichiarata ufficialmente secondo le procedure pertinenti previste dal diritto dell'Unione o nazionale;

Legge sui dati e sicurezza informatica

Esempio

Una grande azienda sanitaria viene presa di mira da un cyberattacco avvenuto tramite ransomware all'interno di un file DICOM di una magnetica. Il file DICOM infetta il computer del medico e poi raggiunge il sistema di archiviazione e comunicazione delle immagini (PACS) dell'ospedale.

Il ransomware prolifera nell'intera rete ospedaliera interrompendo tutte le operazioni e causando l'indisponibilità di dati e servizi. Considerazione (64)

In caso emergenze pubbliche, come ad esempio emergenze sanitarie, emergenze derivanti da disastri naturali, comprese quelle aggravati dal cambiamento climatico e dal degrado ambientale, nonché da gravi catastrofi causate dall'uomo, come ad esempio le gravi violazioni della sicurezza informatica.

in cui l'interesse pubblico derivante dall'uso dei dati supera l'interesse dei titolari dei dati a disporre liberamente dei dati in loro possesso. In tal , i titolari dei dati dovrebbero avere l'obbligo di mettere i dati a disposizione degli enti del settore pubblico, delle autorità di vigilanza e delle autorità di controllo.

Commissione, Banca centrale europea o organismi dell'Unione su loro richiesta. L'esistenza di un'emergenza pubblica deve essere determinata o dichiarata in conformità al diritto dell'Unione o nazionale e sulla base delle procedure pertinenti, comprese quelle delle organizzazioni internazionali competenti. In questi casi, l'ente pubblico dovrebbe dimostrare che i dati oggetto della richiesta non potrebbero essere altrimenti ottenuta in modo tempestivo ed efficace e a condizioni equivalenti, per esempio attraverso la fornitura volontaria di dati da parte di un'altra impresa o la consultazione di una banca dati pubblica.

Articolo 17 Richieste di dati da rendere disponibili

1. Quando richiedono i dati ai sensi dell'articolo 14, un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione devono:
 - a. specificare i dati richiesti, compresi i metadati pertinenti necessari per interpretare e utilizzare tali dati;
 - b. dimostrare che le condizioni necessarie per l'esistenza di un'esigenza eccezionale di cui all'articolo 15 ai fini della quale i dati richiesti sono soddisfatti;
 - c. spiegare lo scopo della richiesta, l'uso previsto dei dati richiesti, compreso, se del caso, quello da parte di terzi ai sensi del paragrafo 4 del presente articolo, la durata di tale uso e, se del caso, il modo in cui il trattamento dei dati personali risponde all'esigenza eccezionale;
 - d. specificare, se possibile, quando si prevede che i dati vengano cancellati da tutte le parti che vi hanno accesso;
 - e. giustificare la scelta del titolare dei dati a cui è rivolta la richiesta;
 - f. specificare eventuali altri enti del settore pubblico o la Commissione, la Banca centrale europea o gli organi dell'Unione e i terzi con cui si prevede di condividere i dati richiesti;
 - g. nel caso in cui vengano richiesti dati personali, specificare tutte le misure tecniche e organizzative necessarie e proporzionate per attuare i principi di protezione dei dati e le garanzie necessarie, come la pseudonimizzazione, e se l'anonimizzazione può essere applicata dal titolare dei dati prima di renderli disponibili;
 - h. indicare la disposizione di legge che attribuisce all'ente pubblico richiedente, alla Commissione, alla Banca centrale europea o all'organismo dell'Unione il compito specifico svolto nell'interesse pubblico per la richiesta dei dati;
 - i. specificare il termine entro il quale i dati devono essere resi disponibili e il termine di cui all'articolo 18, paragrafo 2, entro il quale il titolare dei dati può rifiutare o chiedere la modifica della richiesta;
 - j. fare del proprio meglio per evitare che l'adempimento della richiesta di dati comporti la responsabilità del titolare dei dati per violazione del diritto dell'Unione o nazionale.

Articolo 17 richieste di messa a disposizione dei dati

2. Una richiesta di dati effettuata ai sensi del paragrafo 1 del presente articolo deve:
 - a. essere redatto per iscritto ed espresso in un linguaggio chiaro, conciso e semplice, comprensibile per il titolare dei dati;
 - b. essere specifici per quanto riguarda il tipo di dati richiesti e corrispondere ai dati su cui il titolare dei dati ha il controllo al momento della richiesta;
 - c. essere proporzionati alla necessità eccezionale e debitamente giustificati, per quanto riguarda la granularità e il volume dei dati richiesti e la frequenza di accesso ai dati richiesti;
 - d. rispettare gli obiettivi legittimi del titolare dei dati, impegnandosi a garantire la protezione dei segreti commerciali ai sensi dell'articolo 19, paragrafo 3, e i costi e gli sforzi necessari per rendere disponibili i dati;
 - e. riguardano i dati non personali, e solo se si dimostra che ciò non è sufficiente per rispondere all'eccezionale necessità di utilizzare i dati, ai sensi dell'articolo 15, paragrafo 1, lettera a), richiedere dati personali in forma pseudonimizzata e stabilire le misure tecniche e organizzative da adottare per proteggere i dati;
 - f. info m il titolare dei dati sulle sanzioni che saranno imposte ai sensi dell'articolo 40 dall'autorità competente designata ai sensi dell'articolo 37 in caso di mancato adempimento della richiesta; [...]

Articolo 18 - Conformità alle richieste di dati

1. Il titolare dei dati che riceve una richiesta di messa a disposizione dei dati ai sensi del presente capo mette i dati a disposizione dell'ente pubblico richiedente, della Commissione, della Banca centrale europea o di un organismo dell'Unione senza ingiustificato ritardo, tenendo conto delle necessarie misure tecniche, organizzative e giuridiche.

Veicoli a guida autonoma

Connettività

- Da veicolo a rete (V2N) Da
- veicolo a veicolo (V2V)
- Vehicle-to-Infrastructure (V2I) e Infrastructure-to-Vehicle (I2V) Vehicle-to-
- Person (V2P)
- Da veicolo a dispositivo (V2D) e da veicolo a tutto V2X)

Caratteristiche attuali di Avs

- Fino ad oggi la maggior parte delle funzioni è stata progettata principalmente per assistere i conducenti piuttosto che sostituirli, fornendo avvisi o prendendo il controllo dei veicoli in situazioni limitate.
- In futuro, con AV completamente sviluppati, queste funzioni faranno parte del processo di guida e contribuiranno essenzialmente a sostituire il conducente.

Il ruolo dell'intelligenza artificiale nei veicoli autonomi

- Senso
- Percepire e localizzare la
- rappresentazione della
- scena Pianificare e
- decidere il controllo
-

Tecnologie AI in AV

Riconoscimento degli oggetti

- Rilevamento (localizzazione) e classificazione di oggetti in un'immagine

Segmentazione

- Ad ogni regione viene assegnata un'etichetta per classificarla nelle categorie prescritte

Localizzazione dei veicoli

- Tecnica utilizzata per stimare utilizzando una sequenza di immagini acquisite nel tempo dalla telecamera montata sul veicolo

Tracciamento di oggetti

- Tecnica utilizzata per determinare la dinamica degli oggetti in movimento.

Problemi di sicurezza informatica

☒ Minacce intenzionali

- sfruttamento malevolo delle limitazioni e delle vulnerabilità presenti nei metodi di IA e ML per causare offese e danni intenzionali

☒ Minacce non intenzionali

- effetti collaterali dell'uso benevolo, a causa delle questioni aperte inerenti alla affidabilità, robustezza, limiti e sicurezza degli attuali metodi di IA e ML

Tipo di minaccia	Descrizione	Esempi del mondo reale	Impatti potenziali
Hacking remoto	Accesso non autorizzato al veicolo sistemi via wireless comunicazione	Jeep Cherokee hack 2015)	Controllo del veicolo acquisizione, funzioni di disabilitazione, rischi per la sicurezza
Manipolazione dei sensori	Interferenze con sensori quali LIDAR, radar, telecamere	L'inganno del pilota automatico Tesla (2016)	Falso ostacolo rilevamento, irregolare comportamento, collisioni
Violazioni dei dati	Accesso non autorizzato a dati sensibili memorizzati o trasmessa dal veicolo	Hackeraggio del server del produttore di veicoli elettrici (2020)	Violazioni della privacy, furto d'identità, compromissione del processo decisionale
Attacchi DoS	Sovraccarico dei sistemi del veicolo per interrompere le normali operazioni	Attacchi DDoS alle reti di veicoli e infrastrutture	Degrado delle prestazioni, perdita di connettività, veicolo immobilizzazione

Contromisura	Descrizione	Vantaggi
Sistemi di rilevamento delle intrusioni	Monitoraggio del traffico di rete alla ricerca di attività dannose	Rilevamento delle minacce in tempo reale, identificazione delle anomalie

Crittografia	Sicurezza dei dati in transito e a riposo	Protegge l'integrità e la riservatezza dei dati
Aggiornamenti regolari	Aggiornamenti OTA per software e firmware	Risolve le vulnerabilità e migliora la funzionalità
Protocolli di autenticazione	Garantire solo l'accesso autorizzato ai sistemi del veicolo	Impedisce l'accesso non autorizzato, protegge la comunicazione

Interventi europei

1. 2016, la Commissione europea ha adottato una strategia europea sui sistemi di trasporto intelligenti cooperativi,
2. Nel 2016, gli Stati membri e la Commissione europea hanno lanciato la piattaforma C Roads per collegare le attività di diffusione dei C-ITS,
3. Nel 2018 la Commissione europea ha pubblicato la Strategia dell'UE per la mobilità del futuro.
4. Nel 2019, la Commissione europea ha istituito un gruppo di esperti della Commissione sulla mobilità cooperativa, connessa, automatizzata e autonoma, denominato "CCAM".
5. Nel settembre 2020, rapporto sull'etica dei veicoli connessi e automatizzati
6. Regolamento 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli utenti vulnerabili della strada (regolamento sulla sicurezza generale dei veicoli)

Interventi internazionali: Regolamenti ONU n. 155 e 156

Regolamento ONU n. 155 sulle disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda la sicurezza informatica e il sistema di gestione della sicurezza informatica.

- richiede un certificato di conformità per il sistema di gestione della sicurezza informatica da parte di un costruttore di veicoli per far sì che il suo veicolo sia approvato per l'uso su strade pubbliche.
 - Un approccio sistematico basato sul rischio che definisce i processi organizzativi, le responsabilità e la governance per trattare il rischio associato alle minacce informatiche ai veicoli e proteggerli dai cyberattacchi".
 - Ad esempio, i processi utilizzati per l'identificazione dei rischi per i tipi di veicoli e i processi utilizzati per testare la sicurezza informatica di un tipo di veicolo (ad esempio, i metodi di mitigazione dei diversi rischi di sicurezza informatica, comprese le misure per prevenire e rilevare gli accessi non autorizzati).
- Obiettivo: garantire che nessuno possa accedere in modo non autorizzato al sistema del veicolo.

Regolamento ONU n. 156 relativo alle Disposizioni uniformi in materia di omologazione dei veicoli per quanto riguarda l'aggiornamento del software e la gestione degli aggiornamenti del software

- requisiti sulle modalità di aggiornamento del software del veicolo
 - Certificato di conformità per il sistema di gestione degli aggiornamenti software
 - Si tratta di un approccio sistematico che definisce i processi e le procedure organizzative per soddisfare i requisiti per la consegna degli aggiornamenti software
 - Come ad esempio
 - un processo che consenta di identificare eventuali interdipendenze del sistema aggiornato con altri sistemi un
 - processo per stabilire la compatibilità dell'aggiornamento con la configurazione del veicolo di destinazione

Legislazione dell'UE

Regolamento sulla sicurezza generale dei veicoli 2019/2144

- Entrata in vigore il 6 luglio 2022
- Obiettivi: Introdurre l'obbligo di sistemi avanzati di assistenza alla guida per migliorare la sicurezza stradale e stabilire il quadro giuridico per l'omologazione di veicoli automatizzati e completamente privi di conducente nell'UE.

Regolamento di sicurezza generale del veicolo

(26) La connettività e l'automazione dei veicoli aumentano la possibilità di **accesso remoto non autorizzato ai dati di bordo e di modifica illegale del software via etere**. Per tenere conto di tali rischi, i **regolamenti ONU o altri atti normativi sulla sicurezza informatica dovrebbero essere applicati su base obbligatoria** non appena possibile dopo la loro entrata in vigore.

(27) Le modifiche al software possono cambiare in modo significativo le funzionalità del veicolo. Le regole e i requisiti tecnici armonizzati per le modifiche del software devono essere stabiliti in linea con le procedure di omologazione. Pertanto, i regolamenti ONU o altri atti normativi riguardanti i processi di aggiornamento del software dovrebbero essere applicati su base obbligatoria non appena possibile dopo la loro entrata in vigore. Tuttavia, tali **misure di sicurezza non dovrebbero compromettere gli obblighi del costruttore del veicolo di fornire l'accesso a un sistema completo di informazioni diagnostiche e dati di bordo rilevanti per la riparazione e la manutenzione del veicolo**.

Articolo 4 Obblighi generali e requisiti tecnici

5. I costruttori garantiscono inoltre che i veicoli, i sistemi, i componenti e le entità tecniche siano conformi alle prescrizioni applicabili elencate nell'allegato II con effetto a partire dalle date specificate in tale allegato, alle prescrizioni tecniche dettagliate e alle procedure di prova stabilite negli atti delegati e alle procedure e alle specifiche tecniche uniformi stabilite negli atti di esecuzione adottati a norma del presente regolamento, comprese le prescrizioni relative:

- (a) sistemi di ritenuta, crash test, integrità del sistema di alimentazione e sicurezza elettrica ad alta tensione;
- (b) utenti stradali vulnerabili, visione e visibilità;
- (c) il telaio del veicolo, la frenata, i pneumatici e lo sterzo;
- (d) strumenti di bordo, impianto elettrico, illuminazione del veicolo e protezione dall'uso non autorizzato, compresi gli attacchi informatici;
- (e) comportamento del conducente e del sistema; e
- (f) caratteristiche generali del veicolo

Articolo 11 Requisiti specifici relativi ai veicoli automatizzati e ai veicoli completamente automatizzati

- Oltre agli altri requisiti del presente regolamento e degli atti delegati e di esecuzione adottati a norma dello stesso che sono applicabili ai veicoli delle rispettive categorie, i veicoli automatizzati e i veicoli completamente automatizzati sono conformi alle specifiche tecniche stabilite negli atti di esecuzione di cui al paragrafo 2 che :
 - sistemi che sostituiscono il controllo del veicolo da parte del conducente, tra cui la segnalazione, lo sterzo, l'accelerazione e la frenata;
 - per fornire al veicolo informazioni in tempo reale sullo stato del veicolo e dell'area circostante;
 - sistemi di monitoraggio della disponibilità del conducente;
 - registratori di dati di eventi per veicoli automatizzati;
 - formato armonizzato per lo scambio di dati, ad esempio per il platooning di veicoli multimarca;
 - per fornire informazioni sulla sicurezza agli altri utenti della strada.

Tuttavia, le specifiche tecniche relative ai sistemi di monitoraggio della disponibilità del conducente, di cui al primo comma lettera c), non si applicano ai veicoli completamente automatizzati.

- La Commissione adotta, mediante atti di esecuzione, disposizioni relative a procedure e specifiche tecniche uniformi per i sistemi e gli altri elementi elencati al paragrafo 1, lettere a) a f), del presente articolo e per l'omologazione dei veicoli automatizzati e completamente automatizzati in relazione a tali sistemi e altri elementi, al fine di garantire il funzionamento sicuro dei veicoli automatizzati e completamente automatizzati sulle strade pubbliche.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 13, paragrafo 2.

Internet delle cose

Definizione di IoT

Non esiste una definizione universalmente accettata di Internet degli oggetti (IoT) e i suoi elementi possono variare, compresi la tecnologia, gli strumenti e le applicazioni coinvolte. Secondo l'Unione Internazionale delle Telecomunicazioni, l'IoT è descritta come "un'infrastruttura globale per la gestione delle reti di telecomunicazioni".

società dell'informazione, abilitando servizi avanzati attraverso l'interconnessione di cose (fisiche e virtuali) basate sulle tecnologie dell'informazione e della comunicazione interoperabili esistenti e in evoluzione".

L'ecosistema IoT è costituito da oggetti collegati alla rete tramite sensori, che si interfacciano con il mondo fisico e interagiscono tra loro. Questi oggetti si scambiano informazioni sul loro stato e sull'ambiente circostante senza la necessità di un intervento umano.

Struttura tecnica

La struttura tecnica dell'IoT è tipicamente suddivisa in tre livelli: il **livello di percezione**, che coinvolge i sensori e i dispositivi che raccolgono i dati; il **livello di elaborazione**, che gestisce l'elaborazione dei dati e il processo decisionale; e il **livello di applicazione**, dove i dati elaborati vengono utilizzati per fornire servizi e funzionalità agli utenti.

Architettura tecnica IoT - rischi per la sicurezza

A livello di **informazioni**, i rischi principali includono la garanzia dell'integrità dei dati, la protezione dell'anonimato, il mantenimento della riservatezza e la salvaguardia della privacy.

A **livello di accesso**, le preoccupazioni principali sono il controllo degli accessi, l'autenticazione e l'autorizzazione per garantire che solo gli individui o i sistemi autorizzati possano accedere ai dati e ai servizi.

A **livello funzionale**, l'attenzione si concentra sulla resilienza agli attacchi o ai guasti e sull'abilitazione dell'auto-organizzazione per consentire al sistema di adattarsi a condizioni o minacce mutevoli.

IoT e protezione dei dati

Nei sistemi IoT non esiste una connessione binaria diretta tra un elaboratore di dati e un soggetto interessato. I dati raccolti possono produrre intuizioni preziose, o "frutti", che possono essere complessi sia soggettivamente che oggettivamente. Possono essere raccolti vari tipi di dati, creando una serie di sfide diverse.

Il parere 8/2014 del WP29 sui recenti sviluppi dell'Internet degli oggetti evidenzia diverse preoccupazioni in materia di privacy e protezione dei dati. poste dall'IoT. Si tratta di sfide nuove e tradizionali, amplificate dalla crescita esponenziale dell'elaborazione dei dati. Gli otto problemi principali identificati sono:

1. Mancanza di trasparenza nei sistemi IoT.
2. Il coinvolgimento di vari attori, spesso sconosciuti agli utenti.
3. Perdita di controllo sull'elaborazione dei dati attraverso i dispositivi IoT.
4. Difficoltà nell'ottenere un consenso valido da parte degli utenti, la cui qualità è spesso compromessa.
5. Mancanza di granularità nei servizi IoT, che costringe gli utenti ad accettare tutti gli aspetti dell'elaborazione dei dati o a rifiutare completamente il servizio.
6. La possibilità di trattare un numero di dati superiore a quello necessario per scopo originario.
7. L'utilizzo di dati provenienti da fonti e dispositivi diversi per scopi diversi da quelli originariamente previsti.
8. Rischi di sicurezza nella trasmissione di dati personali tra dispositivi, servizi centrali o altri dispositivi.

Livello di compatibilità

Per il trattamento dei dati è necessario un **consenso specifico e adeguatamente informato**.

Il **Regolamento 1807/2018** sul libero flusso dei dati garantisce la circolazione dei dati all'interno dell'UE proteggendo al contempo la privacy. Il **principio di finalità** prevede che i dati siano utilizzati solo per scopi specifici.

I **limiti di archiviazione dei dati** garantiscono che i dati non vengano conservati più a lungo del necessario.

I **trasferimenti verso paesi terzi** devono essere conformi ai requisiti di protezione dei dati.

L'**identificazione del responsabile del trattamento dei dati** garantisce chiarezza sulle responsabilità.

Privacy by design e sicurezza by design

Standard di responsabilità

- Pseudonimi e riduzione della quantità di dati raccolti
- Consenso a termini di trattamento trasparenti
- Progettazione di politiche sulla privacy
- Trasmissione e recupero sicuro dei dati

Problemi di sicurezza informatica

Articolo 13 Legge sulla resilienza informatica

1. Quando immettono sul mercato un prodotto con elementi digitali, i produttori devono garantire che sia stato progettato, sviluppato e prodotto in conformità ai requisiti essenziali di cui alla parte 1 dell'Allegato I.
2. Ai fini della conformità al paragrafo 1, i fabbricanti effettuano una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali e tengono conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali al fine di ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti di sicurezza e ridurre al minimo l'impatto di tali incidenti, anche in relazione alla salute e alla sicurezza degli utenti.

I **requisiti di sicurezza** includono un approccio basato sul rischio, considerando la triade CIA (Riservatezza, Integrità, Disponibilità), garantendo la minimizzazione dei dati, la resilienza contro gli attacchi DoS, evitando gli effetti di rete, implementando la sicurezza per progettazione con misure di mitigazione,

mantenere un registro delle attività interne e fornire aggiornamenti, anche automatici.

I **requisiti per la gestione delle vulnerabilità** sono anch'essi basati sul rischio e richiedono che i test e gli aggiornamenti di sicurezza siano forniti gratuitamente agli utenti, insieme alla condivisione delle informazioni, in particolare con i produttori di componenti di terze parti.

Privacy by design e sicurezza by design

Interventi sul mercato:

- Impegno di sicurezza di IoT
 - 1. Nessuna password universale: Il prodotto non deve avere una password universale; per il funzionamento saranno necessarie credenziali di sicurezza uniche.
 - 2. Interfacce protette: Tutte le interfacce del prodotto devono essere adeguatamente protette dal produttore.
 - 3. Crittografia comprovata: La sicurezza del prodotto deve utilizzare una crittografia forte, comprovata e aggiornabile, utilizzando metodi e algoritmi aperti e sottoposti a revisione paritaria.
 - 4. Sicurezza per impostazione predefinita: La sicurezza del prodotto deve essere opportunamente abilitata per impostazione predefinita dal produttore.
 - 5. Aggiornamenti software firmati: Il prodotto deve supportare solo aggiornamenti software firmati.
 - 6. Aggiornamenti applicati automaticamente: Il produttore deve agire rapidamente per applicare tempestivamente gli aggiornamenti di sicurezza.
 - 7. Programma di segnalazione delle vulnerabilità: Il produttore deve implementare un programma di segnalazione delle vulnerabilità, che deve essere affrontato in modo tempestivo.
 - 8. Data di scadenza della sicurezza: Il produttore deve essere trasparente sul periodo di tempo in cui saranno forniti gli aggiornamenti di sicurezza.

Responsabilità per i danni dell'IoT

La **responsabilità per danni** è trattata nell'**articolo 82 del GDPR**, che stabilisce la responsabilità per le parti coinvolte nel trattamento dei dati personali. Si coordina inoltre con la **direttiva sulla responsabilità dei prodotti**, che prevede il risarcimento dei danni derivanti da prodotti difettosi.

Responsabilità nell'intelligenza artificiale

La **proposta di direttiva sulla responsabilità per l'IA** mira a migliorare il funzionamento del mercato interno stabilendo norme uniformi per la responsabilità civile non contrattuale per i danni causati dai sistemi di IA. Tra i suoi obiettivi vi sono la promozione di un'IA affidabile, la garanzia che le vittime di danni legati all'IA ricevano una protezione equivalente a quella di cui godono i danneggiati da prodotti e la riduzione dell'incertezza giuridica per le imprese coinvolte nell'IA. In questo modo si eviterà la frammentazione delle norme nazionali sulla responsabilità civile per l'IA.

La direttiva prevede norme sulla responsabilità **extracontrattuale**, il che significa che il risarcimento può essere richiesto indipendentemente dal rapporto contrattuale.

tra la vittima e la parte responsabile. Copre i danni a persone o aziende causati da colpe o omissioni di un fornitore, sviluppatore o utilizzatore di IA in aree quali la salute, la proprietà e la privacy. Tuttavia, esclude la responsabilità legata ai trasporti, la revisione della normativa e l'uso di strumenti di comunicazione.

Direttiva sulla responsabilità per danno da prodotti, legge sui servizi digitali e responsabilità penale.

L'**articolo 4** introduce una **presunzione di causalità**, che semplifica le richieste di risarcimento collegando la non conformità al diritto dell'Unione o nazionale all'output del sistema di IA o alla sua mancata produzione di risultati rilevanti. Se la vittima è in grado di dimostrare la colpa e un probabile nesso di causalità tra le prestazioni dell'IA e il suo comportamento.

il danno, il tribunale può presumere che la non conformità abbia causato il danno, rendendo più facile per le vittime richiedere un risarcimento. Tuttavia, l'onere della prova non è completamente invertito.

Internet delle cose per la salute

IoT

L'ecosistema è costituito da oggetti collegati alla rete tramite sensori, che si interfacciano con il mondo fisico, interagiscono tra loro e si scambiano informazioni sul loro stato e sull'ambiente circostante, il tutto senza l'intervento umano. Questo vale per **dispositivi sanitari**.

Il **livello di percezione** comprende i dispositivi indossabili e impiantati, nonché gli ospedali. Il **livello**

di elaborazione comprende i servizi middleware.

Il livello applicativo comprende servizi di alto livello.

Applicazione del GDPR

Il trattamento dei dati sanitari è definito all'articolo 4(15) del GDPR, dove i dati sanitari sono descritti come "dati personali relativi alla salute fisica o mentale di una fisica, compresa la prestazione di servizi sanitari, che rivelano informazioni sul suo stato di salute". Il considerando 35 chiarisce ulteriormente che i dati sanitari riguardano le condizioni di salute passate, attuali o future dell'interessato.

- Trattamento lecito

art. 9 GDPR

- Trattamento di categorie particolari di dati solo in presenza di una specifica base giuridica: consenso dell'interessato, trattamento dei dati effettuato per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica quando l'interessato si trova nell'incapacità fisica o giuridica di dare il proprio consenso, dati resi manifestamente pubblici dall'interessato, trattamento dei dati finalizzato alla prevenzione o alla medicina del lavoro e anche trattamento dei dati per motivi di interesse pubblico nell'ambito della salute pubblica.

Requisiti di sicurezza Art.

- 32 GDPR 32 GDPR

o Il titolare del trattamento deve "mettere in atto misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio" per proteggere i dati personali da trattamenti non autorizzati o illegali e da perdite, distruzioni o danni accidentali.

- Cosa succede in caso di violazione?

- Decisione CNIL SAN-2022-009, 15 aprile 2022 :

o L'Autorità francese per la protezione dei dati ha imposto una multa amministrativa di 1,5 milioni di euro a un'azienda che tratta dati medici e che non ha rispettato gli articoli 28, 29 e 32 del GDPR.

o La sicurezza dei dati personali non è stata garantita, in quanto sono state riscontrate numerose violazioni tecniche e organizzative in termini di sicurezza: mancanza di una procedura specifica per le operazioni di migrazione dei dati; mancanza di crittografia dei dati personali memorizzati sulla problematica server; assenza di cancellazione automatica dei dati dopo la migrazione all'altro software; assenza di autenticazione da Internet per accedere all'area pubblica del server; utilizzo di account utente condivisi da più dipendenti nell'area privata del server; assenza di una procedura per il monitoraggio e la segnalazione degli avvisi di sicurezza sul server.

Applicazione del regolamento sui dispositivi medici

Regolamento sui dispositivi medici 2017/745

- Art. 2(1) MDR

o Un dispositivo medico è "qualsiasi strumento, apparecchio, dispositivo, software, impianto, reagente, materiale o altro articolo destinato dal fabbricante ad essere utilizzato, da solo o in combinazione, per gli esseri umani a scopo di diagnosi, prevenzione, monitoraggio", previsione, prognosi, trattamento o alleviamento di una malattia; diagnosi, monitoraggio, trattamento, alleviamento o risarcimento di una lesione o di una disabilità; indagine, sostituzione o modifica dell'anatomia o di un processo fisiologico o patologico o stato; e fornire informazioni mediante l'esame in vitro di campioni derivati dal corpo umano, comprese le donazioni di organi, sangue e tessuti, e che non raggiungono l'azione principale prevista per via farmacologica, immunologica o di altro tipo. metabolici, nel o sul corpo umano, ma che può essere assistito nella sua funzione da tali mezzi.

o NB inclusione del "software" tra i tipi di dispositivi medici, sia il software autonomo che il software collegato ad altri software e il software offerto come servizio a un altro dispositivo medico.

Dispositivi/software medici e per il benessere

- Se la finalità è tra quelle elencate, il dispositivo/software si qualifica come dispositivo medico

o art. 2 (12) MDR: lo scopo è indicato dal fabbricante. Pertanto, spetta al fabbricante fornire informazioni sullo scopo del sull'etichetta, nelle istruzioni per l'uso o nel materiale promozionale o di vendita o nelle dichiarazioni.

o I dispositivi IoT che non hanno uno scopo medico non sono soggetti all'MDR. Tuttavia, possono ancora essere utilizzati in medicina quanto raccolgono dati relativi alla salute.

IOMT

- procedura di certificazione che richiede la conformità a criteri minimi essenziali di qualità e sicurezza definiti nell'Allegato I MDR. Procedura di notifica

Art. 87 MDR : In caso di incidente grave, il fabbricante deve segnalare l'incidente alle autorità competenti. 87 MDR: in caso di incidente grave, il produttore deve segnalare l'incidente all'autorità competente.

Art. 2 (65) MDR, un incidente grave è "qualsiasi incidente che direttamente o indirettamente ha portato, avrebbe potuto o potrebbe portare a uno dei seguenti: la

- morte di un paziente, di un utente o di un'altra persona",

- il grave deterioramento temporaneo o permanente dello stato di salute di un paziente, di un utente o di un'altra persona,
- grave minaccia per la salute pubblica.

Cronologia:

- 2 giorni dopo che il produttore ne è venuto a conoscenza, in caso di grave minaccia per la salute pubblica.
- 10 giorni dopo che è stata stabilita/sospettata la relazione causale tra il dispositivo e l'incidente grave in caso di decesso o di grave deterioramento imprevisto dello stato di salute di una persona.
- 15 giorni dopo che è stata stabilita/sospettata la relazione causale tra il dispositivo e l'incidente grave con qualsiasi altro incidente grave.

I produttori devono

- condurre indagini non appena vengono informati che si è verificato un incidente grave
- intraprendere azioni correttive per ragioni mediche o tecniche per prevenire o ridurre il rischio di un incidente grave, ovvero azioni correttive di sicurezza sul campo (FSCA)
 - o la restituzione di un dispositivo al fornitore o un richiamo, la sostituzione di un dispositivo, la modifica di un dispositivo, il retrofit da parte dell'acquirente di un dispositivo.
 - o modifica o cambiamento di design da parte del produttore, distruzione del dispositivo, consigli forniti dal produttore sull'uso del dispositivo, ispezioni/esami raccomandati dall'utente del dispositivo, modifiche del software/firmware del dispositivo, incluso l'aggiornamento del dispositivo.
- Non appena il produttore decide di implementare una di queste misure, gli utenti del dispositivo devono essere informati tramite un avviso di sicurezza sul campo (FSN) per garantire che le azioni richieste siano seguite e completate in modo tempestivo.

Interazione tra GDPR e MDR

L'IoT medicale deve essere conforme allo stesso tempo al GDPR e ai requisiti MDR.

- Gli organismi nazionali di notifica incaricati di verificare la conformità ai requisiti MDR sono chiamati a verificare anche la conformità al GDPR?
- In che misura, ad esempio, la DPIA effettuata dal produttore in qualità di responsabile del trattamento dei dati è sufficiente a dimostrare le misure di sicurezza previste dall'MDR?

Domanda CRA

IoHT sono prodotti con elementi digitali

- Art. 2(68) CRA "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati a distanza, compresi i componenti software o hardware da immettere sul mercato separatamente. 2(68) CRA "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati a distanza, compresi i componenti software o hardware da immettere sul mercato separatamente "".

Il campo di applicazione di CRA non copre i prodotti con elementi digitali che rientrano nella definizione di dispositivi medici IoMT, soggetti ai requisiti di

- sicurezza e protezione MDR.
- IoHT soggetto ai requisiti di sicurezza informatica della CRA Art. 13

CRA. 13 CRA

- Prima di essere immessi sul mercato, i prodotti con elementi digitali devono essere progettati, sviluppati e fabbricati in modo da garantire un livello adeguato di sicurezza informatica.
- I prodotti devono essere forniti senza vulnerabilità note e sfruttabili e devono essere distribuiti in una configurazione predefinita sicura.
- Allegato 1 - Requisiti di sicurezza e gestione delle vulnerabilità

Notifica

- Art. 14 CRA
- Il produttore deve notificare contemporaneamente al CSIRT designato come coordinatore e all'ENISA qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali di cui venga a conoscenza.
 - o una notifica di allarme precoce di una vulnerabilità attivamente sfruttata, senza ritardi ingiustificati e in ogni caso entro 24 ore dal momento in cui il produttore ne viene a conoscenza
 - o a meno che le informazioni pertinenti non siano già state fornite, una notifica di vulnerabilità, senza indebiti ritardi e in ogni caso entro 72 ore dal momento in cui il produttore è venuto a conoscenza della vulnerabilità attivamente sfruttata
 - o a meno che le informazioni pertinenti non siano già state fornite, una relazione finale, entro 14 giorni dalla disponibilità di una misura correttiva o attenuante

Problemi aperti

Tra le **questioni aperte** vi è la necessità di **coordinare la legislazione orizzontale con quella specifica del settore**, ad esempio distinguendo tra dispositivi medici e sanitari e affrontando gli standard generici nel **Cyber Resilience Act (CRA)**.

Il **sovraccarico di notifiche** è un'altra preoccupazione, con problemi quali la sovrapposizione delle tempistiche, le diverse autorità e i diversi requisiti di contenuto delle notifiche.

Cloud computing

Definizione tecnica

Secondo il National Institute of Standards and Technology (NIST) una "capacità di calcolo" si qualifica come "servizio cloud" se presenta le seguenti cinque caratteristiche:

1. Servizio autonomo su richiesta
2. Ampio accesso alla rete
3. pooling delle risorse
4. 'elasticità rapida' e
5. servizio misurato.

Modelli di servizi cloud

- Infrastruttura come servizio, piattaforma come servizio, software come servizio

Tipi di servizi cloud

Cloud privato, cloud comunitario, cloud pubblico, cloud ibrido

Livelli di servizio del cloud

- il livello dei dati, che rappresenta la casa dei dati del cloud computing, con dati memorizzati e dati in transito;
- il livello applicativo, che rappresenta le applicazioni installate che utilizzano le risorse di cloud computing (hardware e software);
- il livello di rete, che rappresenta gli elementi/servizi di rete utilizzati dal nodo di cloud computing, compresi gli elementi di sicurezza responsabili della protezione della rete;
- il livello host, che rappresenta tutti gli elementi che supportano le funzioni di virtualizzazione, come il server virtuale, le macchine virtuali e l'hypervisor.

Cybersecurity nel servizio cloud

Analisi del mercato della cybersecurity nel cloud di ENISA, marzo 2023

"Diverse lacune nel mercato della cybersecurity in-the-cloud emergono a causa degli squilibri nella distribuzione delle funzioni di cybersecurity tra il lato della domanda e quello dell'offerta. Le lacune del mercato sono radicate nelle preoccupazioni relative alla gestione delle varie minacce e alle responsabilità di distribuzione non chiare in merito all'implementazione e alla manutenzione delle funzioni di cybersecurity del cloud".

Gli stakeholder coinvolti nel cloud computing includono il lato della domanda, costituito dagli utenti finali dei servizi cloud, e il lato dell'offerta, che comprende i fornitori di servizi cloud (CSP) e i cloud enabler. Inoltre, le organizzazioni che conducono attività di ricerca e sviluppo (R&S) nel cloud computing e gli enti normativi che supervisionano le attività legate al cloud computing svolgono un ruolo cruciale.

Il rapporto tra cybersecurity e cloud computing è multidimensionale. Le aziende del mercato della cybersecurity contribuiscono al cloud computing offrendo sicurezza dal cloud, sicurezza per l'infrastruttura di cloud computing (ad esempio, protezione dei componenti dello stack) e sicurezza nel cloud, ad esempio garantendo la riservatezza dei dati. D'altro, le aziende del mercato del cloud computing offrono servizi di cloud pubblico, fornitori di software indipendenti e servizi di cloud gestito, oltre a broker di cloud e altre offerte correlate.

Caratteristiche specifiche

Il contratto Cloud include una serie di elementi tecnici che si applicano indipendentemente dal tipo di servizio coperto dal contratto stesso:

1. i dati non sono più memorizzati sui server "fisici" dell'utente, ma sono allocati sui sistemi del fornitore (ad eccezione delle copie locali)
2. l'infrastruttura del fornitore di servizi è condivisa da molti utenti (modello multi-tenant), per cui sono essenziali adeguati livelli di sicurezza
3. la fruizione del servizio avviene via web attraverso Internet, che assume quindi un ruolo centrale per la qualità dei servizi utilizzati ed erogati
4. i servizi che possono essere acquistati dal fornitore di servizi sono su base pay-as-you-go per far fronte a qualsiasi esigenza che possa presentarsi con elasticità e semplificazione sistemi di implementazione (ad esempio, quando è più spazio su disco o più potenza di calcolo).

Definizione dell'operazione di elaborazione e del suo contesto

Dati personali trattati	Informazioni di contatto (e nome del paziente, indirizzo, numero di telefono, indirizzo e-mail), informazioni di contatto dei parenti per i casi di emergenza, numero di assicurazione sociale, appuntamenti medici, risultati di esami medici, patologie, allergie, diagnosi e piani di trattamento (informazioni mediche), informazioni amministrative e finanziarie, informazioni di base, informazioni di base, informazioni di base, informazioni di base, informazioni di base, informazioni di base. informazioni (fatture, documenti di ricovero, ecc.)
Scopo del trattamento	Fornitura di servizi sanitari (diagnosi, trattamento, ricovero), pianificazione del trattamento e fatturazione
Dati dell'interessato	Pazienti, parenti, medici, infermieri
Destinatario dei dati	Medici e infermieri, amministrazione e , sistema sanitario pubblico, pazienti
Elaboratore dati	IaaS Fornitore di servizi cloud

Sfide per la protezione dei dati

Tecniche di privacy by design, Gestione dei dati, Cancellazione dei dati, Portabilità dei dati

Sfide di sicurezza informatica

Controllo degli accessi, audit, autorizzazione, disponibilità, catena della fiducia, catena della responsabilità, conformità, riservatezza, gestione degli incidenti di cybersecurity, identificazione e autenticazione, integrità, multi-tenancy, sicurezza di rete, privacy, archiviazione, trasparenza, visibilità, non ripudio.

Architettura della sicurezza informatica nel cloud computing

Controllo degli accessi	Controlla l'accesso ai dati e sistemi attraverso meccanismi di autenticazione e autorizzazione	Autenticazione e autorizzazione
Crittografia	Converte i dati in un formato codificato per impedire l'accesso non autorizzato, applicato ai dati a riposo e in transito	Applicato a diversi livelli (storage, rete o applicazione)
Backup e ripristino dei dati	Garantire il recupero dei dati in caso di violazione o guasto del sistema, conservati in un luogo sicuro.	Backup dei dati in servizio cloud separato o dati on-premise centro
Sicurezza di rete	Protegge dagli attacchi informatici e dagli accessi non autorizzati.	firewall, IDS/IPS e VPN
Conformità	L'adesione alle normative e agli standard pertinenti, come GDPR e PCI DSS, è fondamentale per una forte sicurezza informatica.	

Sfide di sicurezza informatica

L'acquisizione si riferisce al sequestro e alla raccolta di dati remoti, grandi volumi di dati e dati distribuiti ed elastici potenzialmente collegati all'accusa o all'incidente nell'ambiente cloud.

La conservazione prevede il mantenimento dell'integrità degli artefatti digitali attraverso funzioni di imaging, hashing e duplicazione per garantire che le prove rimangano inalterate.

L'esame è il processo di revisione dei dati forensi raccolti durante la fase di acquisizione per generare input per ulteriori analisi forensi.

L'analisi comporta l'esame dettagliato dei dati, compresa la fusione e la correlazione dei dati, per trarre conclusioni motivate. Il reporting si riferisce alla presentazione dei risultati, documentando i risultati dell'analisi forense.

Legge sui servizi digitali - DSA

Direttiva sul commercio elettronico (Direttiva 2000/31/CE)

Ambito di applicazione: tutti i servizi della società dell'informazione (ISS) stabiliti in uno Stato membro²³ compresi gli intermediari online come i semplici conduit] Obiettivo: contribuire al corretto funzionamento del mercato interno

Principio del paese d'origine: deroga possibile solo sulla base di motivi limitati e di requisiti procedurali
Esenzione di responsabilità limitata per gli intermediari, fatte salve le ordinanze del tribunale [ora sostituito da DSA]

Caratteristiche del DSA

L'obiettivo di questo regolamento è garantire la sicurezza online, ridurre la diffusione di contenuti illegali e dannosi, promuovere un Internet più aperto e trasparente, salvaguardare la libertà di parola e migliorare la protezione dei minori.

Ha un'applicazione orizzontale, che copre tutti i tipi di intermediari online e di contenuti illegali.

Il regolamento è neutrale in quanto l'illegalità è definita dal diritto nazionale o dell'UE, ma è sempre possibile ottenere un provvedimento ingiuntivo in linea con la legislazione nazionale e con le condizioni stabilite nel Digital Services Act (DSA).

Armonizza le esenzioni di responsabilità, assicurando di non attribuire responsabilità per i contenuti, e stabilisce obblighi di due diligence autonomi per i soggetti coinvolti.

Piattaforme online molto grandi	Piattaforme online e motori di ricerca con oltre 45 milioni di utenti nell'UE
Piattaforme online	Mercati online, app store, piattaforme di economia collaborativa, social network...
Servizi di hosting	Servizi cloud, webhosting...
Intermediari	Fornitori di accesso a Internet, registri di nomi di dominio

Avviso e azione

La continuità tra il Digital Services Act (DSA) e la Direttiva sul commercio elettronico si trova negli articoli 4, 5 e 6 del DSA, che corrispondono agli articoli 12, 13 e 14 della Direttiva sul commercio elettronico. Entrambe le serie di articoli fanno una distinzione tra diversi tipi di fornitori di servizi online: mere conduit, caching e hosting. La responsabilità può derivare da qualsiasi tipo di contenuto illegale, indipendentemente dalla sua natura o origine.

La DSA introduce novità, come l'articolo 6, paragrafo 3, che tratta della responsabilità ai sensi della legge sulla protezione dei consumatori, e l'eccezione di responsabilità legata all'adempimento degli obblighi di diligenza.

Giurisprudenza esistente della CGUE

L'ISP deve essere un attore neutrale: nessun ruolo attivo che possa dare all'ISP la conoscenza o il controllo del contenuto (considerando 18).

Il mero conduit, il caching e l'hosting ISP sono diversi= mera elaborazione tecnica e automatica deve essere adattata al tipo di servizi

Giurisprudenza esistente della CGUE

Clausola del buon samaritano - Art. 7 DSA

- L'esenzione di responsabilità si applica ancora in caso di misure volontarie volte a contrastare i contenuti illegali

Controllo pubblico

La progettazione dei sistemi delle piattaforme dà priorità ai rischi e agli interessi della società. Per identificare e affrontare i rischi sociali emergenti viene utilizzato un approccio dinamico. Questo approccio riguarda la progettazione di base di un servizio, compresi i termini e le condizioni, i sistemi algoritmici e le scelte di ottimizzazione. Una solida supervisione è essenziale e comprende audit indipendenti, supervisione regolamentare e controllo pubblico tramite rapporti di trasparenza, accesso ai dati per i ricercatori, consultazione sulle linee guida e coinvolgimento nella valutazione dei rischi e nella progettazione delle misure di mitigazione.

Governance e applicazione

A livello nazionale, il Coordinatore dei Servizi Digitali (DSC) è un'autorità indipendente responsabile del coordinamento con le altre autorità nazionali competenti, nonché della supervisione e dell'applicazione diretta della conformità. Il Comitato europeo per i servizi digitali è un organo ad hoc che si occupa di

gruppo consultivo indipendente, composto da coordinatori nazionali dei servizi digitali, presieduto dalla Commissione e incaricato di fornire consulenza ai DSC e alla Commissione, formulando raccomandazioni. La Commissione europea ha poteri diretti di applicazione della normativa sulle piattaforme online di grandi dimensioni (VLOP) e sui motori di ricerca online di grandi dimensioni (VLOSE), fornisce consulenza sulle controversie transfrontaliere e interviene in seguito alle richieste dei DSC.

Non vi è alcun obbligo legale di comunicare con il pubblico in generale, a meno che la violazione non comporti un rischio elevato per i diritti e le libertà delle persone e la notifica diretta agli interessati sarebbe sproporzionata. In questi si può alla comunicazione pubblica.

La trasparenza delle violazioni dei dati svolge un ruolo fondamentale nel creare fiducia tra gli interessati e i responsabili del trattamento. È anche un aspetto importante del patrimonio di un'organizzazione, in quanto un solido quadro di conformità può accrescere il valore dell'azienda, in particolare in scenari come fusioni o acquisizioni. Inoltre, la trasparenza aiuta a proteggere la reputazione dell'organizzazione dimostrando responsabilità nel trattamento dei dati personali.