ISSN 2704-8012

European Journal of Privacy Law & Technologies

2020/1



G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2020
www.ejplt.tatodpr.eu

CYBERSECURITY, CONCORRENZA, CONTRATTI E CYBER-RISK

CYBERSECURITY, COMPETITION, CONTRACTS AND CYBER-RISK

Domenico Fauceglia

Avv. Ph.D. at Università di Roma Tor Vergata

Abstract:

Insieme con il cambiamento climatico, la sicurezza delle reti e dei sistemi informativi costituisce un'emergenza mondiale. Dxiverse sono le sfide che, nei prossimi anni, l'Italia dovrà affrontare al fine di promuovere la cultura sulla sicurezza cibernetica. In questo delicato contesto, l'articolo contribuisce a descrivere la disciplina europea e interna in tema di cybersecurity, nonché le problematiche relative all'attività di impresa e alla gestione dei rischi presenti nel cyberspace.

Together with climate change, the security of networks and information systems constitutes a global emergency. There are several challenges that Italy will have to face in the coming years in order to promote the culture of cybersecurity. In this delicate context, the article helps to describe the European and national discipline on the topic of cybersecurity, as well as the issues relating to business activities and the management of risks present in cyberspace.

Parole chiave: sicurezza informativa; concorrenza; Direttiva NIS.

Key-words: *cybersecurity; competition; NIS Directive.*

Summary: 1. La *Cybersecurity,* Industria 4.0 e smart city. – 2. La Dirtettiva NIS e *cyber* – sicurezza nell'attività di impresa – 3. La disciplina giuridica interna della *cybersecurity.* – 4. *Cyber-risk* e nuovi prodotti assicurativi. – 5. Il *Cybersecurity Act.* – 6. L' armonizzazione delle diverse leggi sulla *Cybersecurity* e il GDPR. – 7. Le certificazioni sulla sicurezza.

1. La *Cybersecurity,* Industria 4.0 e *Smart city*

Il fenomeno della *cybersecurity* ha fatto ingresso nel nostro ordinamento con la Direttiva europea NIS 2016/1148/UE (*Network and Information Security*) volta a stabilire le misure per la realizzazione in Europa di un ambiente digitale sicuro e affidabile [1].

Per evidenziare l'importanza della disciplina della cybersecurity, occorre osservare il continuo procedimento di trasformazione digitale dei più importanti settori della nostra economia. L' evoluzione digitale sta conducendo ad una duplice realtà: reale e virtuale. Diverse imprese, negli ultimi anni, hanno preferito investire sul digitale e sulle nuove tecnologie che permettono un maggiore incremento di efficienza, affidabilità e sicurezza nella produzione di beni, erogazione dei servizi e nella gestione dell'attività d'impresa.

A ciò si aggiunge che l'internet delle cose (Iot) permette una migliore connessione di oggetti del mondo fisico nonché un miglior collegamento e migliore comunicazione (intesa come scambio di dati) tra il mondo virtuale e il mondo reale.

In questo contesto, rilevano le nuove Industrie 4.0 e le *Smart cities c*he operano su due livelli: il livello fisico (la fabbrica o la città) con le sue diverse infrastrutture (i macchinari nel caso della fabbrica, le strade, le reti, i mezzi di trasporto, ecc., nel caso della città) e il livello *cyber c*he, contenendo una rappresentazione "virtuale" delle cose materiali, ne permette il controllo e la gestione attraverso le nuove tecnologie.

Obiettivo del livello cyber è quello di monitorare, in modo continuo, lo stato delle infrastrutture fisiche, adattandole alle esigenze della produzione o dei cittadini al fine di coniugare efficienza e qualità dei prodotti e dei servizi.

In questi termini, si percepisce maggiormente il pericolo o il danno che potrebbe derivare da un possibile attacco *cyber.*

2. La Direttiva NIS e cyber – sicurezza nell'attività di impresa

La Direttiva europea NIS – recepita in Italia con il Decreto Legislativo 18 maggio 2018, n. 65 – affronta, per la prima volta a livello europeo, il tema della *cyber security* e definisce le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei

[1] Cfr. A. CONTALDO, F. PELUSO, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa 2018; A. CONTALDO, D. MULA, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* Pisa 2020; B. PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Milano 2020.

sistemi informativi; tra l'altro, la notifica degli incidenti di sicurezza informatica subiti [2]. L'incremento della digitalizzazione e della connettività – anche grazie all'avvento dell'Internet degli oggetti ("*Internet of things*" o *IoT*) – espone le reti e i sistemi informativi a maggiori rischi connessi alla *cyber*-sicurezza, ne deriva che la società è sempre più vulnerabile alle minacce informatiche. Considerati i maggiori pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori, si è rilevata necessaria l'emanazione del Regolamento 2019/881/UE, conosciuto come *Cybersecurity act* [3].

Prima di procedere all'analisi della disciplina relativa alla cybersecurity, si rende doverosa una precisazione sul concetto di cybersicurezza, oggi intesa come «*insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*» (art. 2, Reg. 2019/881/UE).

Anche se la disciplina della *cybersecurity* sia attuale, il termine *Cyber Security* non è nuovo. Esso era già diffuso negli anni Novanta del secolo scorso, ma solo negli ultimi anni sta assumendo contorni maggiormente precisi.

Una delle prime definizioni di *cybersecurity* è riportata all'interno della norma ISO/IEC 27000:2014 che la descrive come: «*quella pratica che consente ad un'entità (un'organizzazione, un cittadino, una nazione, ecc.) di proteggere i propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni, dalle minacce che arrivano dal cyberspace*» (ISO/IEC, 2014).

In quest'ottica, le finalità della Direttiva NIS e del più recente *Cybersecurity act* sono dirette a garantire un livello minimo di "igiene informatica" e a ridurre al minimo possibile l'esposizione delle reti, dei servizi e dei sistemi di comunicazione elettronica, a rischi derivanti da minacce informatiche.

Invero, la direttiva NIS del 6 luglio 2016, al fine di prevenire rischi e incidenti informatici, offre una disciplina diretta a regolare il controllo e le condotte nei casi di incidente (cioè ogni evento pregiudizievole per la sicurezza, art. 4 n.

---

[2] Con il Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Come si avrà modo di notare nel prosieguo, il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

[3] L'opportunità di regolare la disciplina con regolamento era già stata manifestata da G. BRUNO (*La* cybersecurity *nel sistema del diritto europeo*, in *Diritto delle Comunicazioni*, a cura di G. Bruno, Torino 2019, p. 470), il quale si era già posto in senso critico alla scelta del legislatore euro-unionale di adottare una direttiva, in particolare l'A. ritiene che «proprio per l'importanza della materia ed in considerazione del carattere sovranazionale di fenomeni che si svolgono su contesti di carattere globale, sarebbe stato opportuno per il legislatore comunitario operare con lo strumento tecnico del Regolamento anziché con quello della Direttiva al fine di evitare spazi di discrezionalità applicativa in grado di alterare nell'effetto pratico le normali dinamiche di un mercato fondato sulla concorrenza».

7 Dir. NIS) e di rischio (cioè ogni evento potenzialmente pregiudizievole, art. 4 n. 9 Dir. NIS) delle reti e dei sistemi informativi.

Per rete e sistema informativo si intende, ai sensi dell'art. 4 n. 1, una rete di comunicazione elettronica e, dunque, i sistemi di trasmissione e le apparecchiature che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse [4].

Ancora, per rete e sistema informativo, si intendono anche qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico dei dati digitali; nonché i dati digitali, trattati estratti o trasmessi per mezzo di reti o dispositivi.

In particolare, la cybersecurity è «*l'insieme delle misure che riducono il rischio che la confidenzialità, l'integrità e la disponibilità dei dati, siano essi in transito o statici, vengano impattate negativamente dalle minacce provenienti dal cybercrime che incombono su di essi e che sono amplificate dalla pervasività e complessità delle interconnessioni di rete attuali e future*» [5].

L'esigenza di rendere maggiormente sicure le reti e i servizi informativi, nonché l'esigenza di una disciplina in caso di rischi e incidenti informatici, sono volte anche ad assicurare il normale esercizio delle attività economiche.

Diversamente le imprese, esponendosi eccessivamente a rischi e danni, inevitabilmente verrebbero colpite da gravi perdite finanziarie conseguenti ad una impossibilità di gestione aziendale nonché ad una diffusa sfiducia dei consumatori e degli utenti. Tali pericoli, insomma, creerebbero particolari danni all'economia europea.

Non solo, la sicurezza delle reti e dei sistemi informativi – svolgendo un ruolo di primaria importanza nell'agevolare i movimenti transfrontalieri di beni, servizi e persone – si rileva essenziale per l'armonioso funzionamento del mercato interno.

Come si è anticipato, la disciplina è diretta a tutelare le reti e i sistemi informativi – ossia le reti di comunicazione elettronica, qualsiasi dispositivo o insieme di dispositivi interconnessi, nonché i dati digitali ivi trattati (cfr. art. 4, n. 1) Direttiva 2016/1148/UE) – è sostanzialmente diretta a tutelare i dati, anche personali, ivi contenuti.

Per tali ragioni, le tre caratteristiche del dato che devono esser salvaguardate sono rappresentate dalla c.d. "***CIA Triad***" (da *Confidentiality, Integrity, Availability*), in particolare:

---

[4] Sul punto si rimanda a D. FAUCEGLIA, *Il contratto di utenza telefonica*, Milano 2020, p. 13 ss.

[5] Y. I. AGOSTINI, *Le basi di Cybersecurity per il giurista*, in Ziccardi, *Tecnologia e diritto*, vol. I, Milano 2019, p. 158

a) la **disponibilità** (*Availability*) che misura l'attitudine di un'entità o sistema ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante;

b) la **confidenzialità** (*Confidentiality*), ossia la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti;

c) l'**integrità** (*Integrity*), ossia la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali (involontarie) oppure effettuate volontariamente da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione *ex novo* di dati ed informazioni.

In questi termini, dal momento che l'informazione costituisce una utilità (dunque un bene in senso giuridico *ex* art. 810 cod. civ.) e dal momento che, oggigiorno, la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati.

Invero, occorrerebbe chiarire la natura di dato digitale. In questo contesto, l'art. 810 cod. civ. non fornisce una definizione universale di bene giuridico, limitandosi a descrivere il procedimento di oggettivazione attraverso cui una certa entità acquista rilievo per l'ordinamento giuridico come bene giuridico [6].

Una determinata entità (come i dati digitali conservati, estratti e trattati per mezzo di reti e dispositivi *ex* art. 4 lett. 1 Direttiva NIS) suscita determinati interessi (anche non tipizzati) che possono essere soddisfatti solo con l'attribuzione di un certo diritto soggettivo e delle relative tutele [7].

In quest'ottica, si potrà sempre fare ricorso all'analogia ed estendere il procedimento appropriativo della proprietà, come era già stato fatto tempo fa per il *software* ed il *know-how* ed ora anche per le criptovalute e il *cloud computing.*

In ragione degli interessi tutelati, si giustificano precisi obblighi a carico delle imprese in materia di sicurezza delle reti e sistemi informativi.

Si badi, però, non bisogna confondere la disciplina della tutela dei dati personali con la disciplina della sicurezza delle informazioni *tout court* le quali, seppure siano riservate e confidenziali, nulla hanno che vedere con dati personali [8]. Ebbene,

---

[6] Sul punto O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, Milano 1982, p. 39 e ss.; D. MESSINETTI, *Oggettività giuridica delle cose incorporali*, Milano 1970, p. 105, secondo cui «quella dei beni è una vera e propria qualificazione e non una semplice classificazione secondo un ordine determinato e caratteri comuni».

[7] R. NICOLÒ, *Istituzioni di diritto privato*, Milano 1962, p. 3 s.

[8] Per tali ragioni, esiste a livello internazionale la norma ISO 27001 finalizzata alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Lo standard indica i requisiti di un adeguato sistema di gestione della sicurezza delle informazioni (SGSI; in inglese: *Information*

il trattamento dei dati personali, pur essendo richiamato tra i primi articoli della Direttiva NIS (in particolare art. 2), riguarda solo ed esclusivamente la disciplina dei dati personali. Infatti, l'art. 2 della Direttiva Nis, nel distinguere i due *corpora* normativi, precisa che «il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE». D'altro canto, la legge sulla privacy infatti non impone alcuna protezione per informazioni prive di dati personali.

La *cybersecurity* si occupa esclusivamente della protezione delle reti e i dei sistemi informativi al fine di tutelare la *CIA triad* dei dati ivi trattati.

In relazione alla protezione degli *asset* informatici, quest'ultima è costituita da un complesso di misure di prevenzione e di protezione, tese ad assicurare: *a*) l'accesso protetto e controllato ai dati, a garanzia della confidenzialità delle informazioni trattate (proprietà di *riservatezza*); *b*) la consistenza dei dati, intesa come completezza e correttezza degli stessi (proprietà di *integrità*); *c*) l'accesso ai dati nei tempi e nei luoghi previsti (proprietà di *disponibilità*).

Le proprietà di riservatezza, integrità e disponibilità dei dati costituiscono l'assunto base sul quale vengono svolte tutte le successive valutazioni di sicurezza. Tali proprietà sono in genere affiancate anche dalla proprietà di *non ripudio*, ovvero dalla possibilità di attribuire un dato a un mittente o proprietario ben identificato.

Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: robustezza del *software* di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati.

Con la sicurezza informatica, si enfatizzano qualità di *resilienza (*resistenza a un attacco informatico)*, robustezza* e *reattività* che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance (attacchi *cyber*).

Al fine di valutare la sicurezza informatica (quindi, il pericolo di attacchi interni o esterni dannosi per gli *asset* informatici) è necessario individuare le eventuali:

---

security management system o ISMS) finalizzato a una corretta gestione dei dati dell'azienda. Una fase indispensabile di ogni pianificazione della sicurezza è la valutazione del rischio e la gestione del rischio. Le organizzazioni possono far certificare ISO 27001 il proprio SGSI. In particolare, lo standard ISO/IEC 27001 (Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti) è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa. La versione più recente della norma è la ISO/IEC 27001:2017 (pubblicata il 30 marzo 2017), che non è altro che la versione 2013 con due modifiche (emesse dall'ISO nel 2014 e 2015): 1) requisito A.8.1.1: l'inventario, la classificazione e trattamento degli "asset" riguarda ora anche le "informazioni" cui gli asset sono associati; 2) requisito 6.1.3: la Dichiarazione di Applicabilità deve specificare se sono implementati o meno i "controlli necessari", e non solo i controlli riferiti all'Annex A.

a) minacce;

b) vulnerabilità, ossia i punti deboli del sistema riguardo ai quali le misure di sicurezza sono ridotte o, addirittura, assenti;

c) e rischi, ossia la probabilità che un'azione (o una inerzia) possa comportare la perdita di fatti o, comunque, un evento indesiderabile.

In termini pratici, le misure di *cybersecurity* si focalizzano su come comportarsi per prevenire un incidente di sicurezza (ai fini della prevenzione risulta essenziale una dettagliata analisi del rischio [9]) e come comportarsi nel caso un tale incidente si verifichi.

Il procedimento di analisi del rischio inizia con la preventiva identificazione dei beni da proteggere per poi valutare le possibili minacce in termini di potenziali danni e perdite (gravità). Una volta stimato il rischio delle reti e dei servizi informativi, si decidono quali misure di sicurezza adottare (c.d. piano di rischio). L'analisi del rischio tipicamente precede la fase di messa in esercizio del sistema informatico.

Giova ripetere che spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, ma piuttosto dai dati in essi contenuti: la sicurezza informatica deve quindi preoccuparsi di impedire l'accesso non solo agli utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a specifiche operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati.

Le violazioni possono essere molteplici, vi possono essere: a) tentativi non autorizzati di accesso a zone riservate; b) furto di identità digitale o di file riservati; c) utilizzo di risorse che l'utente non dovrebbe potere utilizzare.

La protezione dagli attacchi informatici viene ottenuta agendo a due livelli principali:

1) ***sicurezza fisica***. Per *sicurezza passiva* (fisica) normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia il complesso di misure volte ad impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

2) ***sicurezza logica***. Per *sicurezza attiva* (logica) si intendono le tecniche e

[9] Ciò è anche confermato nelle linee guida (cybersecurity framework) emanate dal National Institute of Standards and Technology (NIST, agenzia del Governo degli Stati Uniti d'America) che prevedono i seguenti macro-processi: identifica (*identify*); proteggi (*protect*); rileva (*detect*); rispondi (*respond*); ripristina (*recover*).

gli strumenti mediante i quali le informazioni e i dati (nonché le applicazioni) di natura riservata sono resi sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autenticato o non autorizzato possa modificarli (integrità) [10].

Le misure di sicurezza passiva e attiva sono tra loro complementari. Entrambe sono indispensabili per raggiungere un livello di sicurezza adeguato degli asset informatici (in termini di prevenzione e di protezione) e sono tese ad assicurare la "*CIA Triad"* dei dati ivi contenuti.

3. La disciplina giuridica della cybersecurity

Come si è anticipato, il D. Lgs. 18 maggio 2018 n. 65 – attuativa della direttiva NIS 2016/1148/UE che lascia spazi di libertà agli «Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi», art. 2, lett. *a*) – individua, invece, i soggetti competenti a dare una prima attuazione alla *cyber* difesa europea.

Al fine di conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, l'art. 2, co. II, D.Lgs. 2018 n. 65, prevede:

a) l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;

b) la designazione delle autorità nazionali competenti e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di monitoraggio e intervento in caso di incidenti, emissione di preallarmi e analisi dinamica dei rischi;

---

[10] Per intendere cosa sia un sistema di sicurezza logico, occorre fare riferimento all'esperienza media di qualsiasi utente. È noto che gli sviluppatori di *software*, sin dalla progettazione dei programmi, devono attuare misure in grado di assicurare l'efficienza d'uso del programma e le sue capacità di "sopravvivenza" in caso di attacchi esterni e di errori più o meno critici. La sicurezza dei programmi è da due caratteristiche fondamentali: a) *Safety* (sicurezza): una serie di accorgimenti atti ad eliminare la produzione di danni irreparabili all'interno del sistema; b) *Reliability* (affidabilità): prevenzione da eventi che possono produrre danni di qualsiasi gravità al sistema. In quest'ottica, un software (o programma) è tanto più sicuro quanto minori sono le probabilità che si verifichi un malfunzionamento dello stesso. Gli errori di programma non nocivi, come ad esempio gli *spyware* e il *buffer overflow*, hanno la caratteristica di non modificare i file di sistema e non recare danno alle caratteristiche del sistema stesso. Quelli nocivi – come i virus informatici, i Trojan o il Cracking – possono essere contrastati solo con determinate misure di sicurezza logica: 1) *Update* e *Upgrade* di sistemi operativi con *patch* di sicurezza; 2) *Antivirus* che consente di proteggere il proprio *personal computer* da *software* dannosi conosciuti come *virus*. Ma, un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale.

c) il rispetto di obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonché dell'incremento della fiducia tra di essi;

e) la partecipazione nazionale alla rete CSIRT nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.

Ebbene, come rileva dall'art. 2, la normativa si applica anzitutto agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

Gli OSE sono organizzazioni pubbliche o private che forniscono servizi essenziali per la società e l'economia nei settori dell'energia, dei trasporti, bancario, infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile, delle infrastrutture digitali e del campo sanitario [11].

Ai sensi dell'art. 4 co. 2 D.Lgs. 18 maggio 2018, n. 65, i criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti: a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Affinché un incidente possa considerarsi produttivo di effetti negativi rilevanti sulla fornitura del servizio, le autorità competenti NIS (ossia i Ministeri a capo di ogni settore [12]) considerano i seguenti fattori intersettoriali:

---

[11] Ciò in conformità con la direttiva (UE) 2016/1148 ha stabilito obblighi concernenti le capacità nazionali nel campo della cybersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, fornitura e distribuzione di acqua potabile, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di *cloud computing* e mercati online).

[12] Le Autorità competenti NIS sono responsabili dell'attuazione del D.Lgs. 18 maggio 2018 n.65 con riguardo ai settori e ai servizi ivi riportati e vigilano sull'applicazione del decreto a livello nazionale esercitando altresì poteri ispettivi e sanzionatori. Ai sensi dell'art. 7 D.Lgs. n. 65 del 2018, sono designate quali Autorità competenti NIS per i settori e sottosettori di e per i servizi: a) il Ministero dello sviluppo economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali; b) il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada; c) il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca D'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze; d) il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il trami-

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

I FSD, invece, sono le persone giuridiche che forniscono servizi di *e-commerce, cloud computing o motori di ricerca.* È importante notare che non rientrano nella direttiva gli FSD con meno di 50 dipendenti e un fatturato o bilancio annuo inferiore ai 10 milioni di euro (il legislatore richiama nuovamente il concetto di "microimpresa").

Tali soggetti (tanto gli OSE quanto gli FSD):

– devono adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi;

– devono prevenire e minimizzare l'impatto degli incidenti di sicurezza delle reti e dei sistemi informativi;

– sono tenuti a notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, sulla continuità e sulla fornitura del servizio, informandone anche l'Autorità nazionale competente (c.d. NIS).

L'Italia, mediante il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio, ha identificato gli operatori di servizi essenziali operanti sul nostro territorio. Si tratta in totale di 465 realtà, tra pubbliche e private, delle quali per motivi di sicurezza non sono stati forniti i nomi; verranno resi noti quando il livello di *cyber* difesa di ognuno sarà giudicato all'altezza.

La **notifica degli incidenti** dovrà essere effettuata dagli OSE e FSD al CSIRT (*Computer Security Incident Response Team* italiano), che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale).

I soggetti giuridici non identificati come OSE e che non sono FSD possono

---

te delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza; e) il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

inoltrare su base volontaria al CSIRT (quest'ultimo istituito presso la Presidenza del Consiglio dei Ministri) notifiche degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati.

Infatti, l'intento della Direttiva NIS è quello di favorire la più ampia diffusione di una cultura nel campo della cyber security e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni tra gli apparati di *cyber* difesa che gli stati potranno introdurre per far fronte ai crescenti rischi in campo *cyber security*. Solo una puntuale condivisione delle minacce ha permesso e permetterà agli organi di contrasto ed alle autorità nazionali ed europee di accrescere il livello di consapevolezza ed istradare azioni di contrasto efficaci.

In relazione a tali esigenze si spiega la istituzione della rete CSIRT. In questi termini, occorre chiarire che – siccome la sicurezza delle reti e dei sistemi informativi è oggetto di interesse di ogni Stato membro – risulta necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti di sicurezza.

Ebbene, la responsabilità di garantire la sicurezza della rete e dei sistemi informativi incombe in larga misura agli operatori di servizi essenziali e ai fornitori di servizi digitali degli Stati membri. In quest'ottica, come previsto dall'art. 12 Direttiva NIS, al fine di contribuire allo sviluppo della fiducia fra stati membri e di promuovere una cooperazione operativa rapida ed efficace, è istituita la rete CSIRT che svolge i compiti di scambio di informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT.

IL CSIRT italiano, a cui sono attribuite le medesime funzioni del *Computer Emergency Response Team* (CERT), svolge diversi compiti in ambito *cyber security* che se attuati possono realmente contribuire ad incrementare il livello di sicurezza europeo:

– la definizione di procedure per la prevenzione e la gestione degli incidenti informatici;

– la ricezione delle notifiche di incidente con obbligo di informare il Dis, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;

– la fornitura, al soggetto che ha effettuato la notifica, di informazioni che possono facilitare la gestione efficace dell'evento;

– l'informazione degli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite.

In ultimo, l'aspetto incoraggiante sotto il profilo collaborativo è il fatto che il

CSIRT deve identificare forme di collaborazione, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practice.*

Il modulo per la notifica è unico sia qualora la notifica avvenga su base obbligatoria che facoltativa [13]. Le informazioni richieste sono tante ma non tutte necessarie.

Qualora obbligatoria, la mancata comunicazione espone inevitabilmente le società al rischio sanzione per omessa comunicazione. In attuazione della Direttiva, infatti, l'Italia ha previsto un regime sanzionatorio secondo cui potranno essere irrogate sanzioni amministrative fino a 150.000 euro per gli OSE e fino a 125.000 euro per i FSD.

L'aspetto che tuttavia preoccupa è il numero di comunicazioni, obbligatorie o facoltative, che potrebbe essere necessario effettuare in caso di incidente di sicurezza: all'interessato e al Garante privacy (in caso di *data breach*), al CSIRT, all'Organismo di vigilanza, al management aziendale e in alcuni contesti alla Banca d'Italia e alla BCE.

4. *Cyber-risk* e nuovi prodotti assicurativi

Posto che assume sempre più rilievo la *Cyber Risk,* intesa come ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e per i sistemi informatici, nel mercato assicurativo si stanno sempre più diffondendo prodotti assicurativi relativi al rischio informatico che coprono i soli rischi e non anche le sanzioni.

Nei contratti di assicurazione, volti a coprire il *cyber-risk,* accanto alle prestazioni dell'assicurato e dell'assicuratore, è necessaria l'esistenza del rischio che se non è mai esistito o ha cessato di esistere prima della conclusione del contratto determinerebbe la nullità del contratto (art. 1895 cod. civ.).

Invero, sotto il profilo funzionale, l'assicurazione intesa quale operazione economica attua sempre un trasferimento di un rischio dalla sfera dell'assicurato (che in tal caso è un OSE o FSD) a quella dell'assicuratore, il quale provvederà alla neutralizzazione dello stesso mediante il suo inserimento in una massa di rischi omogenei secondo i principi della tecnica assicurativa.

Come si è già notato, il rischio cibernetico è un rischio di tipo operativo che è associato alle perdite economiche inflitte ad una organizzazione dalla mancata

[13] In attesa che il complesso meccanismo prenda forma basterà collegarsi al sito www.csirt-ita.it. Ad oggi per una eventuale notifica di incidenti potrà essere utilizzato il modulo disponibile nella sezione Modulistica del sito. Che dovrà essere firmato digitalmente e inviato in forma cifrata all'indirizzo e-mail: notifica.nis[at]csirt-ita.it.

confidenzialità, disponibilità di integrità di informazioni e sistemi informativi, propri o di terzi.

Il rischio cybernetico può essere accidentale o deliberato a seconda che l'incidente si verifichi per cause non imputabili ai soggetti coinvolti, ad esempio nel caso dello spegnimento di un *server;* sarebbe, invece, un rischio deliberato nell'ipotesi di eventi che derivano da condotte volontarie di soggetti che hanno lo scopo di raggiungere degli obiettivi personali di varia natura, come nel caso di un attacco cibernetico da parte di un *hacker* che intende sottrarre i dati sensibili.

Invero, l'assicurazione che copre la *Cyber Risk* ha una certa importanza in termini: 1) controllo del rischio in caso di sospetti di incidenti informatici e *data breach;* 2) la polizza assicurativa si pone come ausilio ad una più agevole gestione dell'impresa nella crisi cibernetica (essa accompagna l'impresa a ridurre i danni derivanti da sanzioni, interruzione di esercizio, fermo dell'attività).

La *Cyber Insurance* si pone come strumento volto a minimizzare i rischi e i danni informatici, ma non copre eventuali sanzioni amministrative (si veda Reg. IVASS n. 38/2018 che prevede l'implementazione di un sistema di monitoraggio sistematico per identificare tempestivamente incidenti e valutare la resilienza al *cyber risk*) [14].

5. *Cybersecurity Act*

Il 7 giugno 2019 la Gazzetta Ufficiale della UE ha pubblicato il regolamento comunemente denominato *Cybersecurity Act* o "Regolamento sulla *cybersicurezza"* (Regolamento (UE) 2019/881 del 17 aprile 2019), entrato in vigore il 27 giugno 2019.

Questo intervento, a livello di quadro generale sulla sicurezza del *Web* in ambito unionale, completa precedenti azioni della UE in questo ambito, come la direttiva NIS (direttiva (UE) 2016/1148) ed il *General Data Protection Regulation* (Regolamento 2016/679/UE).

L'Unione europea ha approvato il cosiddetto *Cybersecurity Act* che introduce un complesso quadro normativo al fine di armonizzare maggiormente la politica di *resilienza* da attacchi cibernetici in tutto il territorio europeo. A questo fine, il regolamento interviene su due versanti principali:

[14] A tal riguardo giova richiamare l'art. 32 del citato Reg. IVASS che dispone che deve essere notificato all'Ivass ogni evento che possa ragionevolmente comportare, o abbia già comportato cambiamenti sostanziali dell'attività e dei risultati del sistema di "governance", del profilo di rischio o della condizione finanziaria e di solvibilità dell'impresa.

• il primo, rinnovando il ruolo ed il mandato conferito all'agenzia europea ENISA che, d'ora in poi, sarà un centro di competenza permanente sul tema e fornirà supporto agli Stati membri nell'implementazione delle relative politiche di sicurezza;

• il secondo, mediante la istituzione di un processo di certificazione europeo sulla sicurezza cibernetica, riconosciuto da tutti gli Stati membri.

Invero, come rileva dal *Considerando* n. 65 del Regolamento 2019/881/UE, la certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti TIC (ossia elementi di reti e sistemi informativi), servizi TIC (ossia la trasmissione, conservazione e recupero di informazioni attraverso la rete o i sistemi informativi) e processi TIC (ossia le attività volte a programmare o sviluppare un prodotto o un servizio TIC) e nell'accrescere la fiducia da parte degli utenti negli stessi.

Il mercato unico digitale, in particolare l'economia dei dati e l'*Internet d*egli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un determinato livello di cibersicurezza. Invero il sistema di certificazione è già ampiamente utilizzato nei settori delle automobili connesse e automatizzate, dei dispositivi medici elettronici, dei sistemi di controllo per l'automazione industriale e delle reti elettriche intelligenti.

Orbene, il recente regolamento costituisce un ulteriore passaggio verso una maggiore sicurezza del mondo digitale europeo che aveva già registrato precedenti importanti sia col GDPR sia con la direttiva NIS.

L'ambiente informatico è divenuto strategico per la gestione e lo sviluppo delle nostre società; reti, sistemi informativi e servizi di comunicazione elettronica (tecnologie dell'informazione e comunicazione, cosiddette "TIC") «svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica (...) in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno».

L'incremento della digitalizzazione e della connettività – anche grazie all'avvento dell'Internet degli oggetti ("*Internet of things"* o IoT) – «comporta maggiori rischi connessi alla cibersicurezza» mentre di converso, «la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione». "Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), fino ai gestori delle infrastrutture critiche.» [Considerando (1-3)].

La politica di supporto alla sicurezza cibernetica in ambito UE è stata perseguita con una pluralità di interventi tra cui i principali sono il GDPR e la direttiva NIS, pur con le dovute differenze connesse ai diversi contesti di riferimento.

Sebbene l'ambito applicativo del GDPR sia confinato al dominio dei dati personali, il tema della sicurezza è affrontato dal regolamento in modo strategico sotto il profilo quantitativo e qualitativo.

Dal punto di vista quantitativo, la definizione molto ampia di "dato personale" fa rientrare nel dominio applicativo del GDPR la quasi totalità del patrimonio informativo di cui necessita un'organizzazione, qualsiasi sia il settore di appartenenza.

Sotto il profilo qualitativo, la sicurezza delle informazioni è un principio di liceità del trattamento dei dati personali, nel senso che l'uso degli stessi non può ritenersi lecito se sprovvisto di un adeguato sistema di misure tecnico-organizzative di salvaguardia.

Per il GDPR, pertanto, un utilizzo non sicuro di dati personali è illecito e suscettibile di sanzioni e di provvedimenti inibitori, con gravi ripercussioni sul business aziendale. La declinazione di dettaglio di questo principio si ritrova nella prescrizione dell'articolo 32 che impone al titolare del trattamento di adottare misure tecnico-organizzative adeguate al rischio nonché nella regolamentazione del processo di violazione dei dati personali ("*data breach"*), la più completa disciplina sul tema in ambito unionale (artt. 33 e 34).

6. L' armonizzazione delle diverse leggi sulla *Cybersecurity* e il GDPR

La Direttiva NIS (UE 2016/1148) costituisce il primo atto giuridico della UE sulla sicurezza cibernetica – oggetto dell'*Alert d*el 5 luglio 2018, cui si rinvia. Essa affronta il tema della sicurezza nelle infrastrutture critiche e della disciplina di eventuali *data breach* in tali ambiti, istituendo «i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri».

La direttiva NIS, come indica il termine, è basata sullo strumento giuridico della "direttiva" unionale anziché su quello del "regolamento" per cui, diversamente da quest'ultimo, si indirizza agli Stati membri e deve essere recepita da questi tramite atti normativi nazionali.

Per l'Italia, la direttiva NIS – lasciando impregiudicata la possibilità di ciascun stato membro di adottare misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza (*Considerando* n. 8 Direttiva NIS) – è stata recepita tramite il decreto legislativo n. 65/2018.

In questi termini, differentemente dal GDPR, la direttiva NIS:

• non si riferisce a qualsiasi tipologia di organizzazione ma unicamente ai gestori di infrastrutture critiche (cioè quelli dell'energia e dei trasporti, quello bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) ed ai fornitori di servizi di-

gitali (precisamente, mercato online, motori di ricerca online, servizi di cloud computing).

• impone agli operatori dei servizi essenziali e ai fornitori dei servizi digitali di notificare solo gli incidenti che abbiano un impatto rilevante sui servizi forniti (in tal caso, si tiene conto del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all'area interessata dall'incidente), sebbene anche nel contesto NIS, vi sia l'obbligo di adottare le misure per prevenire e minimizzare gli impatti degli incidenti nonché di individuare le misure tecniche e organizzative relative alla gestione dei rischi.

A ciò si aggiunge il *Cybersecurity act* del 17 aprile 2019. Lo strumento giuridico del regolamento europeo è stato prescelto sulla base della considerazione che «*le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali*» mentre gli attacchi informatici avvengono spesso attraverso le frontiere tanto da richiedere un intervento normativo uniforme.

Gli obiettivi del *Cybersecurity Act s*ono quelli di:

• creare un quadro normativo di riferimento – omogeneo a livello UE – a supporto della resilienza agli attacchi informatici

• creare un mercato unico della sicurezza cibernetica per prodotti, servizi e processi

• accrescere la fiducia dei consumatori nelle tecnologie digitali.

7. Le certificazioni sulla sicurezza

Il *Cybersecurity Act* sostituisce il precedente regolamento (UE) 526/2013 con il quale si era dato l'ultimo rinnovo al mandato dell'ENISA, sino al 2020.

Il regolamento sulla cybersicurezza si compone essenzialmente di due parti:

1. quella in cui vengono specificati il ruolo ed il mandato della rinnovata agenzia europea sulla sicurezza cibernetica ("ENISA") (artt. 1-45)
2. quella in cui si istituisce un sistema europeo per la certificazione della sicurezza informatica di dispositivi, prodotti e servizi digitali (artt. 46-65).

L'Agenzia europea per la sicurezza delle reti e dell'informazione ("ENISA") era già stata istituita nel 2004, con mandato limitato sia sotto il profilo della competenza (prevalentemente consultiva, per contribuire all'obiettivo generale di garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nella UE) sia sotto quello temporale (in quanto, nonostante i ripetuti rinnovi, il mandato all'agenzia sarebbe infine scaduto nel 2020).

Il *Cybersecurity Act* trasforma l'ENISA in un'agenzia permanente – un vero centro di competenza europeo sulla cybersecurity – ampliandone le competenze che includono:

• l'attività di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri nonché nello sviluppo e nell'attuazione delle politiche comunitarie

• un ruolo di primo piano nella gestione del sistema di certificazione introdotto dal regolamento, mediante la predisposizione di schemi europei per la certificazione sulla sicurezza cibernetica che saranno poi adottati dalla Commissione mediante atti di esecuzione.

L'ulteriore principale intervento del *Cybersecurity Act* consiste nell'aver introdotto un quadro normativo per la **certificazione sulla sicurezza** in internet di valenza unionale per assicurare un approccio comune sul mercato interno dell'Unione e, da ultimo, per migliorare la sicurezza cibernetica dei prodotti digitali incrementando la fiducia riposta dai consumatori nel mercato digitale [15].

Anche in questo caso, la certificazione introdotta dal Cybersecurity Act lascia impregiudicata «l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità» al GDPR «dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento» anche nel caso che le operazioni di trattamento siano integrate nelle TIC [v. Considerando (74)].

La certificazione sulla sicurezza cibernetica disciplinata dal Cybersecurity Act parte da schemi di certificazione che – come detto – sulla base di un quadro complessivo di regole comunitarie, vengono realizzati dall'ENISA, sono approvati dalla Commissione con atti di esecuzione, e conseguentemente vengono riconosciuti in tutti gli Stati membri; in questo modo si viene a modificare la situazione precedente che annoverava schemi di certificazione specifici per prodotti e sistemi TIC, esistenti presso singoli paesi ma non riconosciuti a livello transnazionale: si veda, ad esempio, il caso dei contatori intelligenti (o "*smart meters"*) i cui produttori sono sottoposti a distinti processi di certificazione in Francia, Gran Bretagna e Germania. Quindi, il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi ma definisce un quadro regolatorio per la loro creazione. Una volta adottato uno schema di certificazione europeo, le aziende volontariamente potranno presentare domanda di certificazione dei propri prodotti, servizi o processi agli organismi di certificazione nazionali (in Italia, l'OCSI, Organismo di Certificazione della Sicurezza Informatica);

[15] Per una interessante lettura in tema di certificazioni di qualità, si cfr. E. BELLISARIO, *Certificazioni di qualità e responsabilità civile*, Milano 2011.

salvo che la certificazione di sicurezza non venga espressamente richiesta come obbligatoria per specifici prodotti o servizi da eventuali norme di settore.

Gli obiettivi di maggiore interesse per la certificazione della sicurezza sono:

• appurare che i sistemi, servizi o processi siano in grado di proteggere i dati dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita;

• verificare che siano in grado di proteggere i dati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità;

• che l'accesso di persone, programmi o macchine sia limitato esclusivamente ai dati, ai servizi o alle funzioni per i quali questi dispongono dei diritti di accesso;

• che siano state individuate e documentate le dipendenze e vulnerabilità note, che sia possibile registrare a quali dati, servizi o funzioni è stato effettuato l'accesso, in quale momento e da chi;

• che sia possibile ripristinare tempestivamente la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in caso di incidente fisico o tecnico;

• che siano utilizzati criteri di "security by design" per la progettazione di prodotti e servizi, e "by default", in modo che tali prodotti implementino le impostazioni più sicure, ed infine che il software e l'hardware dei prodotti TIC siano costantemente aggiornati per mezzo di meccanismi protetti.

Tenendo conto che non tutti i sistemi, processi e servizi hanno lo stesso profilo di rischio, il Cybersecurity Act prevede tre livelli di certificazione differenti (art. 52 commi 5, 6 e 7):

• Un livello di affidabilità "di base" per il quale il produttore/fornitore può ricorrere all'autocertificazione, ove prevista; in questa ipotesi può bastare un riesame della documentazione tecnica, o attività di valutazione sostitutive di effetto equivalente intese a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici.

• Un livello di affidabilità "sostanziale" per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo i rischi noti alla cybersicurezza ed i rischi di incidenti ed attacchi informatici commessi da soggetti che dispongono di abilità e risorse limitate. Le attività di valutazione comprendono almeno un riesame per verificare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti o servizi attuino correttamente le necessarie funzionalità di sicurezza.

• Un livello di affidabilità "elevato", per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati, commessi da attori che dispongono di abilità e risorse significative.

Le attività di valutazione comprendono: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC attuano correttamente le necessarie funzionalità di sicurezza allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione.

I certificati europei sulla sicurezza informatica non attestano o garantiscono che un prodotto o servizio certificato in base ad un determinato schema accreditato sia sicuro bensì che lo stesso risponda agli specifici requisiti definiti nello schema. I certificati così rilasciati saranno riconosciuti in tutti gli Stati membri dell'Unione, facilitando sia gli affari degli operatori che agiscono a livello transnazionale sia la fiducia e consapevolezza degli acquirenti circa il livello di sicurezza certificato.

Obiettivo del legislatore tramite la certificazione europea sulla sicurezza è quello di promuovere la sicurezza informatica sin dalla fase iniziale di progettazione e sviluppo dei prodotti TIC e di quelli di consumo che costituiscono gli *IoT* ("***security by design***"). Questo consentirà agli utenti di conoscere il livello di sicurezza dei prodotti/servizi scelti assicurando che le misure di sicurezza siano verificate in modo indipendente. Le organizzazioni dovrebbero configurare i TIC da loro progettati «in modo da garantire un livello di sicurezza superiore che dovrebbe consentire al primo utente di ricevere una configurazione predefinita con le impostazioni più sicure possibili («sicurezza predefinita»), riducendo al contempo l'onere in capo agli utenti di» doverlo essi stessi configurare in modo adeguato. La sicurezza predefinita dovrebbe essere possibile senza necessità di «conoscenze tecniche specifiche o di un comportamento non intuitivo da parte dell'utente, e dovrebbe funzionare in modo semplice e affidabile quando attuata».