LUISS

Dipartimento di GIURISPRUDENZA

Cattedra di Diritto dell'Unione Europea

LA CYBERSECURITY NELL'UNIONE EUROPEA: TUTELA DEI DATI PERSONALI E CRIMINALITÀ INFORMATICA IN TEMPO DI PANDEMIA

RELATORE
Chiar.mo Prof. **Giacomo BIAGIONI**

_____

CORRELATORE
Chiar.ma Prof. ssa **Angela DEL VECCHIO**

_____

CANDIDATO
Roberto TIBALDI

Matr. 153993

_____

ANNO ACCADEMICO 2020/2021

Indice

«L'Europa sarà forgiata dalle sue crisi e sarà

la somma delle soluzioni trovate per risolvere tali crisi».

*Jean Monnet, (*1954)

INTRODUZIONE

L'avvento delle tecnologie digitali ha rappresentato una svolta epocale per il mondo del diritto interno e sovranazionale. Oggi assistiamo ad un'ulteriore fase di cambiamento dei nostri sistemi socio-economici dal momento che l'evoluzione digitale ha cambiato il modo in cui viviamo generando un nuovo spazio di interazione, il c.d. *cyberspace,* come parte integrante della vita personale e sociale di ognuno di noi.

Se da un lato, però, lo sviluppo tecnologico ha offerto opportunità di progresso, dall'altro si è trasformato in un terreno fertile e appetibile per nuove tipologie e modalità di condotte penalmente rilevanti.

L'incremento delle opportunità legate alle ICT è accompagnato da un parallelo incremento delle vulnerabilità per cui gli attacchi informatici e la criminalità informatica aumentano in tutta Europa sia come numero, sia come livello di sofisticazione.

A livello internazionale, il Vecchio Continente sembrerebbe svolgere un ruolo marginale nella competizione in ambito di ricerca e sviluppo tecnologico che invece vede Stati Uniti e Cina in prima linea.

Ad ogni modo, l'UE si mostra coinvolta e interessata alla crescente digitalizzazione, attenta a non creare un disequilibrio geopolitico preoccupante, partecipe nelle sfide e consapevole dei pericoli che potrebbero minare la sicurezza su vari livelli.

La pandemia, tuttavia, ha fatto emergere con maggiore evidenza tutti i rischi legati alla cybersicurezza marcando un'accelerazione del processo di digitalizzazione della nostra società. A tal proposito, la Commissione europea ha presentato la strategia che pone al centro delle sfide da affrontare proprio la cybersecurity. La strategia europea sulla cybersecurity, costituisce parte integrante della Strategia per la Sicurezza 2020-2025 (EU Security Union Strategy), adottata a luglio 2020 dalla Commissione Europea, per indirizzare l'azione nei settori prioritari in cui l'UE può costituire un valore aggiunto rispetto agli sforzi nazionali. L'obiettivo è quello di affrontare sia la resilienza informatica sia quella fisica delle entità europee, delle reti e delle infrastrutture critiche, per affermare la leadership in materia di norme e standard internazionali nel cyberspazio. Un cyberspazio

globale, aperto e sicuro, fondato sullo stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici.

Nel concetto di "criminalità informatica" rientrano proprio quei fatti criminosi che possono essere commessi attraverso uno spazio virtuale, la rete o c*yberspace.* Si tratta, in sostanza, di comportamenti lesivi di interessi giuridici rilevanti che sono riconducibili ai cd. "reati informatici".

Tuttavia la "criminalità informatica" non rappresenta una categoria definita giuridicamente, né possiamo asserire che esiste una definizione riconosciuta a livello internazionale di "cybercrime" o "computer crime", nonostante compaia in varie fonti sovranazionali ed europee.

Nel presente studio, quindi, verrà presentato inizialmente, il cammino evolutivo che ha portato, attraverso un'elaborazione giurisprudenziale, all'affermazione del diritto alla tutela della vita privata tramite il riconoscimento di tale diritto nella Carta dei diritti fondamentali. Verranno esaminate, per quanto concerne l'Unione europea, la legislazione vigente, la giurisprudenza principale e la natura del diritto al rispetto della vita privata.

Partendo dalla evoluzione storica, si esamineranno le norme introdotte da fonti primarie e di diritto derivato nell'ordinamento giuridico dell'Unione Europea. Tra gli interessi emersi con l'evoluzione tecnologica e cibernetica vanno evidenziati proprio la riservatezza, la privacy e il diritto alla protezione dei dati personali, nozioni simili ma che non risultano coincidenti. Il fenomeno della digitalizzazione e della disponibilità di dati su supporto informatico assume particolare rilevanza e delicatezza lì dove i dati e le informazioni raccolte risultano particolarmente sensibili. Si pensi ad esempio, ai dati e alle informazioni relative alla salute, all'orientamento sessuale, alla religione o alle convinzioni politiche.

Il concetto di privacy in passato è stato a lungo assimilato alla riservatezza. Tuttavia, i concetti di riservatezza e privacy da un lato e quello di protezione dei dati dall'altro, come anticipato, si riferiscono a situazioni giuridiche differenti e non sovrapponibili.

La privacy riguarda l'obbligo di tutelare l'inviolabilità o l'uso illecito di tutti quei dati che compongono l'identità di un individuo, la sua sfera personale, sociale, politica

sanitaria, giudiziaria etc. La riservatezza riguarda il diritto alla non violabilità della propria sfera privata. È uno dei diritti fondamentali sanciti dalla costituzione della Repubblica italiana. Può essere intesa come il diritto a una "vita intima" riconducibile al sistema dei diritti della personalità.

Vedremo come questa, con l'aumento delle attività nel Cyberspace, ha trovato una sua declinazione nella "riservatezza informatica" che viene identificata come «*potestà di escludere terzi e di essere garantiti contro intrusioni indesiderate ed interferenze potenzialmente dannose o comunque non consentite, per salvaguardare un proprio 'spazio informatico' libero, autonomo e sicuro, in cui possa svolgersi senza impedimenti la propria personalità, che opera tramite relazioni ed attività dislocate nella rete*»[1] .

La cd. "riservatezza informatica" ha una portata più ampia, distinta dalla "sicurezza informatica". La riservatezza, oltre a proteggere da accessi abusivi nel domicilio informatico, sia ideale che fisico, in cui si trovano i dati informatici relativi alla persona, garantisce anche la «*sicurezza e l'esclusività dell'accesso, della gestione e della disponibilità del suo spazio informatico, o meglio cibernetico, vale a dire delle risorse informatiche […] contro ogni interferenza e danneggiamento (essendo l'interesse meritevole di tutela comprensivo della confidenzialità, sicurezza e dunque libertà delle azioni ed elaborazioni, anche solo potenziali o future, realizzabili nel 'proprio' ambito esclusivo*)» .

Questi nuovi interessi, quindi, sono stati rapidamente messi a repentaglio dall'evoluzione tecnologica, motivo per cui si è reso necessario un intervento europeo sulla regolazione della materia. Il 24 maggio 2016, infatti, è entrato in vigore il Regolamento n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tale Regolamento, noto anche come GDPR (General Data Protection Regulation), entrato in vigore il 25 maggio 2018, è stato reso attuativo, in Italia, dal D.lgs n. 101 del 10 agosto 2018, entrato in vigore il 19 settembre 2018.

[1] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, Padova 2013, pp. 59-60.

Il Regolamento UE 2016/679, al considerandum n. 6, precisa che «*la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali*[2]*. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*».

Il Regolamento ha novellato il cd. Codice della Privacy di cui al d.lgs. n.196 del 2003 e successive modificazioni. Il Codice della Privacy, pertanto, risulta essere il frutto delle integrazioni apportate dal Regolamento europeo n. 679 del 2016 e del d.lgs. n. 101 del 2018. Verranno qui descritte, dunque, le principali sfide che i processi di digitalizzazione offrono alla tutela del diritto al rispetto della vita privata, individuando gli strumenti previsti dall'ordinamento giuridico dell'Unione europea per garantire una protezione appropriata. La ricerca interesserà l'individuazione e l'esegesi delle norme UE, sia di diritto primario, sia di diritto derivato, sulla tutela dei dati personali e della riservatezza delle informazioni.

Il punto di forza della tesi, dunque, con una elaborazione storica, normativa e giurisprudenziale, non è quello di fornire un'asettica descrizione della strategia europea nel settore. Non una pura ricerca, ma una trattazione di natura teorico-applicativa coerente con gli obiettivi didattici del corso e particolarmente attinente alla mia esperienza professionale, attraverso un osservatorio "privilegiato." Nell'ambito di un tirocinio, avviato presso il Parlamento Europeo a Bruxelles, a partire dal mese di settembre del 2020, infatti, ho avuto modo di svolgere un periodo di formazione in un ambiente lavorativo di alto profilo istituzionale che mi ha consentito di arricchire il percorso di studi di un'importante

[2] T. TESSARO, C*ome cambia la trasparenza amministrativa dopo il Gdpr e il nuovo decreto privacy,* Maggioli, Rimini, 2019, pp.126,127.

esperienza internazionale, di carattere pratico, finalizzata anche alla ricerca per la preparazione della tesi di laurea.

In questo elaborato vedremo come la cybersicurezza sia divenuta un presupposto imprescindibile per un'Europa digitale e connessa. Lo studio affronta la questione della cybersecurity, quale esigenza per la crescita economica e sociale, attraverso l'analisi delle iniziative intraprese a livello di Unione europea e cercheremo di comprendere come UE e Italia si stanno dotando degli strumenti tecnici e normativi indispensabili alla gestione del fenomeno. L'Unione europea interviene con un ruolo di riferimento per le iniziative nazionali mentre l'Italia sulla base del Quadro strategico nazionale per la sicurezza dello spazio cibernetico e del relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Nella prima parte, verrà quindi esaminato il rischio cibernetico al fine di comprendere come la cultura normativa europea stia davvero investendo sulla valutazione di tale minaccia per implementare misure di sicurezza adeguate e funzionali. Un focus diretto, dunque, sulla normativa europea per affrontare il tema del digitale nel contesto geopolitico europeo e internazionale dal punto di vista delle imminenti sfide e opportunità a livello globale. Lo stato di emergenza ha confermato anche l'importanza di preparare l'UE per il c.d. decennio digitale in cui l'Europa mira a dare maggior impulso alle imprese e ai cittadini in un futuro digitale incentrato sulla persona, più sostenibile e più prospero. Del resto, la crisi indotta dal Covid-19 ha reso l'economia dell'UE più dipendente che mai dalla rete e dai sistemi informatici con servizi sempre più interconnessi.

La salute pubblica resta materia di competenza principalmente statale, poiché in virtù dei Trattati istitutivi e stata attribuita all'Unione europea una competenza di tipo "concorrente" legata a determinati aspetti della sanità pubblica, connessi alla gestione di problemi comuni nonché una competenza per svolgere azioni mirate a sostenere, coordinare o completare l'azione degli Stati membri. Per questo motivo, come del resto espressamente statuito dall'art. 168, par. 7, TFUE, ogni Stato membro definisce autonomamente la predisposizione e l'organizzazione del sistema sanitario, nonché l'assegnazione delle risorse ad esso destinate ed è responsabile della gestione dei servizi sanitari e dell'assistenza medica.

Nel secondo capitolo l'obiettivo è quello di esaminare i crimini informatici e l'illecito utilizzo dei dati. Si cercherà di individuare i rischi reali con un riferimento alla metodologia condivisibile di gestione del rischio che aziende e organizzazioni internazionali dovrebbero sviluppare a seguito dell'evoluzione tecnologica, vista la facilità di duplicazione, memorizzazione, trasferimento e trattamento automatizzato dei dati digitali.

È opportuno passare in rassegna le singole fattispecie incriminatrici, che risentono del difficile problema dell'individuazione del locus *commissi delicti* che pone inevitabilmente un problema a carattere sovranazionale. Nonostante l'UE abbia, in materia penale, una competenza indiretta, l'art 83 TFUE prevede che il Parlamento Europeo e il Consiglio possano stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale tra cui terrorismo, criminalità informatica, criminalità organizzata e riciclaggio di denaro.

Il modello della c.d. società digitale, infatti, ha spinto i vari Stati ad introdurre nuove figure di illeciti, i c.d. computer crimes, che risentono dell'aterritorialità della rete.

Tra i principali computer crimes della disciplina italiana figura l'accesso abusivo ad un sistema informatico o telematico, ai sensi dell'art. 615-ter c.p. che punisce chiunque "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo". L'articolo è inserito all'interno del codice penale dalla legge n. 547 del 23 dicembre 93, al fine di contrastare i fenomeni degli attacchi informatici da parte degli hackers, dando così seguito alla Raccomandazione del Consiglio di Europa del 1989, che equipara il domicilio informatico a quello fisico.

Verranno poi esaminati casi più recenti di cronaca, anche con riferimenti bibliografici di articoli di quotidiani e riviste di attualità, testimonianza di come la minaccia globale della criminalità informatica sia aumentata sia come numero che come gravità di casi.

Poiché s'intende approfondire la tematica attraverso un'analisi critica e comparata e un approccio interdisciplinare, nel quarto capitolo viene presentata un'indagine empirica articolata e sviluppata attraverso ricerca delle fonti, raccolta dei dati, elaborazione ed analisi.

L’attenzione si focalizzerà su un’esamina comparativa realizzata utilizzando un campione di dati strutturati per incrementarne l'usabilità e l’accessibilità. Le informazioni su cybercrime o reati on line contro la persona permetteranno di valutare le tendenze nel corso del tempo. Vogliamo così approfondire le tecniche più sfruttate dai cyber-criminali nel corso della pandemia, a livello europeo, facendo emergere come il cybercrime, ma anche la disinformazione ad opera di fakenews online siano tra i fenomeni che maggiormente si sono sviluppati negli ultimi due anni. Sarà importante comprendere gli effetti immediati derivanti da campagne di phishing, ransomware, malware o più semplici truffe online.

I PARTE:

UE E CYBERSECURITY, NUOVO APPROCCIO STRATEGICO

CAPITOLO PRIMO

IL RAPPORTO TRA CYBER SECURITY E PROTEZIONE DEI DATI PERSONALI

SOMMARIO: 1.1 La tutela dei dati come diritto fondamentale: art.8 della Carta dei diritti fondamentali dell'Unione europea e art. 16 TFUE. – 1.2. Dal Codice Privacy al GDPR. – 1.2.1 L'evoluzione della normativa. – 1.3 La nuova strategia europea di cybersecurity e il GDPR: quali interazioni. – 1.4 Direttiva NIS e Cybersecurity Act: due baluardi UE per la sicurezza nazionale – 1.5 Mandato e nuove sfide dell'ENISA (Agenzia dell'Unione Europea per la cybersicurezza).

1.1 La tutela dei dati come diritto fondamentale: art.8 della Carta dei diritti fondamentali dell'Unione europea e art. 16 TFUE

La protezione dei dati personali e il rispetto della vita privata costituiscono diritti fondamentali della persona umana riconosciuti dall'ordinamento europeo. Solo a partire dagli anni Novanta, con l'entrata in vigore del Trattato di Maastricht, ha trovato un positivo riconoscimento il principio in base al quale l'Unione promuove e tutela i diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), firmata a Roma il 4 novembre 1950. La tutela dei diritti fondamentali, dunque, ha un passato piuttosto recente nell'ambito dell'ordinamento giuridico dell'UE[3].

Tuttavia, già prima dell'entrata in vigore dei Trattati istitutivi[4], la Corte di Giustizia era più volte intervenuta, anche in assenza di una espressa e specifica previsione normativa,

[3] V. SALVATORE *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato Unione Europea,* Studio EPRS | Servizio Ricerca del Parlamento europeo Unità Biblioteca di diritto comparato PE 628.243 – Ottobre2018 IT, Segretariato generale del Parlamento europeo.

per affermare la necessità di tutelare i diritti fondamentali dell'individuo al fine di conseguire gli obiettivi istituzionali assegnati alle Comunità europee.

Da allora, il sistema approntato dall'Unione si è notevolmente evoluto e raffinato, dapprima attraverso l'adozione della Carta dei diritti fondamentali[5], proclamata una prima volta a Nizza il 7 dicembre 2000 e una seconda volta, in una versione adattata, dal Parlamento Europeo, dalla Commissione e dal Consiglio il 12 dicembre 2007, per venire poi recepita dal Trattato istitutivo dell'Unione europea con l'attribuzione del valore di fonte di rango primario, aprendo la strada alla firma del Trattato di Lisbona.

La Carta rappresenta una pietra miliare nell'evoluzione della tutela dei diritti a livello europeo[6], in quanto marca il passaggio dal loro riconoscimento in via pretoria all'espressa individuazione di carattere legislativo. Il ruolo stesso della Corte di Giustizia, così, è stato riportato «nell'ambito consolidato del rule of law»[7]. Al momento della sua prima proclamazione, in realtà era controverso quale valore giuridico si dovesse riconoscere alla CDFUE[8].

Sul trattamento dei dati personali un ideale punto di partenza può essere offerto dalla sentenza Stauder[9] del 1969 che rappresenta una delle prime pronunce nelle quali la Corte si

---

[4] V. SALVATORE, Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato, op.cit.

[5] La Carta dei diritti fondamentali dell'Unione europea (CDFUE), nota come Carta di Nizza. Nel rispetto dei poteri e delle funzioni dell'UE e del principio della sussidiarietà riafferma i diritti così come risultano, in particolare, dalle tradizioni costituzionali e dagli obblighi internazionali comuni dei paesi dell'UE, dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dalle Carte sociali adottate dall'UE e dal Consiglio d'Europa e dalla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. Conferisce visibilità e chiarezza ai diritti fondamentali e contribuisce a creare certezza del diritto nella UE.

[6] M. CARTABIA*, L'ora dei diritti fondamentali nell'Unione Europea*, in I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Bologna, Il Mulino, 2007, p. 15.

[7] G. DEMURO, *La Carta dei diritti*, in Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea, A. Lucarelli, A. Patroni Griffi (a cura di), Napoli, Edizioni Scientifiche Italiane, 2009, p. 232

[8] A tal proposito A. BARBERA, *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di Giustizia*, in Rivista AIC, n. 4/2017, p.3 ss.

[9] Sentenza del 12 novembre 1969, Stauder, 29/69, EU:C:1969:57.

è fatta carico del compito di tutelare i diritti fondamentali della persona, in quanto parte dei principi generali del diritto, sia pure nei limiti della loro compatibilità con la struttura e le finalità della allora Comunità economica europea.

Quanto alla Carta, la giurisprudenza della Corte di giustizia[10] ha chiarito che, come si desume dall'art. 51, par.1, della Carta − dove si stabilisce, ai fini dell'individuazione dell'ambito di applicazione, che le sue disposizioni si applicano agli Stati membri "*esclusivamente nell'attuazione del diritto dell'Unione*" le disposizioni della Carta sono soltanto parametri di legittimità degli atti dell'Unione, degli atti nazionali che ai primi danno attuazione, nonché di quegli atti nazionali che, a giustificazione dell'introduzione di una deroga agli obblighi imposti dai Trattati, invocano l'esigenza di tutelare un diritto fondamentale. Esse quindi non hanno efficacia diretta negli ordinamenti interni degli Stati aderenti alla UE, come ha affermato anche la Corte costituzionale[11] .

Il dibattito sul valore giuridico della Carta di Nizza ha subito un nuovo impulso il 1° dicembre 2009, con l'entrata in vigore del Trattato di Lisbona[12]. Questo ha modificato l'art. 6 TUE[13], conferendole il rango di diritto primario dell'Unione. La natura costituzionale del contenuto della CDFUE, inoltre, è stata anche affermata dalla Corte costituzionale italiana[14].

Tuttavia, l'attenzione rivolta dall'Unione europea e dal Consiglio d'Europa alla tutela dei dati personali tuttavia, risale a prima della Carta di Nizza: fondamentali al riguardo le

[10] V. sentenze 5 ottobre 2010, McB, C-400/10; 12 novembre 2010, Estov, C-339/10; 15 settembre 2011, Gueye e Salmerón Sánchez, C-483/09 e C 1/10; Grande Sezione, 26 febbraio 2013, Åkerberg Fransson, C-617/10.

[11] Cort.Cost. sentenza n. 80/2011, n. 303/ 2011 e n. 210 /2013).

[12] M. BIGNAMI, *Costituzione, Carta di Nizza, CEDU e legge nazionale: una metodologia operativa per il giudice comune impegnato nella tutela dei diritti fondamentali*, in Rivista AIC, n. 1/2011, p. 14 ss.

[13] M. PEDRAZZI, *Artt. 6-7 TUE*, in Commentario breve ai trattati dell'Unione europea, F. POCAR, M.C. BARUFFI (a cura di), II edizione, Padova, Cedam, 2014, p. 35 ss.

[14] 14 Sentenze n. 269/2017 e 20/2019. La Corte ha sostenuto che la CDFUE «costituisce parte del diritto dell'Unione dotata di caratteri peculiari in ragione del suo contenuto di impronta tipicamente costituzionale».

disposizioni contenute nella Convenzione di Strasburgo del 1981 per quanto riguarda il Consiglio d'Europa e le norme introdotte con la direttiva 95/46/CE per l'Unione europea[15].

La convenzione n. 108, firmata a Strasburgo, aperta all'adesione anche di Stati non membri del Consiglio d'Europa, infatti, nacque dall'esigenza di tutela delle persone a seguito del moltiplicarsi di tecnologie dell'informazione e comunicazione a partire dagli anni '60. La Convenzione, è stata oggetto di un processo di modernizzazione, completato con l'adozione, il 18 aprile 2018, del Protocollo di modifica detto anche 'Convenzione 108+' del testo della Convenzione per modernizzarla e fornire un quadro giuridico più consono ad un'epoca in cui le violazioni del diritto alla protezione dei dati costituiscono una importante priorità.

Il protocollo introduce innovazioni rilevanti come l'obbligo di comunicare le violazioni dei dati (data breach) e il rafforzamento del principio di minimizzazione dei dati, e di trasparenza dell'elaborazione. Richiede anche il rispetto del principio di privacy by design, introducendo ulteriori tutele nell'ambito dei trattamenti algoritmici, come il diritto di ottenere informazioni sulla logica alla base dell'elaborazione dei dati. Essa riguarda tutti i tipi di trattamenti, compreso quelli derivanti da sicurezza nazionale e difesa (a differenza del GDPR), tranne i trattamenti operati da persone fisiche nell'esercizio di attività puramente personali e domestiche[16].

Dunque, i principali strumenti legislativi in materia di protezione dei dati sono la Carta dei diritti fondamentali dell'Unione europea dove gli articoli 7 e 8 riconoscono il rispetto della vita privata e la protezione dei dati personali come diritti fondamentali strettamente correlati, ma distinti e il Consiglio d'Europa con la Convenzione 108 del 1981

[15] Direttiva n. 95/46/ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (Pubblicata sulla GUCE n. L 281 del23.11.1995). Prima del GDPR, rappresentava il principale strumento normativo a tutela delle persone fisiche in materia di trattamento dei dati personali, mirava a sostenere la libera circolazione delle informazioni nell'ambito UE, con un ruolo fondamentale per gli scambi commerciali. Ha permesso l'abbattimento delle frontiere nell'ambito dell'Unione europea, contribuendo a creare le condizioni per la realizzazione del free flow of data al centro dell'agenda europea, come strategia per la creazione del Digital Single Market, ossia la cosiddetta "Strategia per il Mercato unico digitale europeo".

[16] https://protezionedatipersonali.it/convenzione-108-consiglio-europa

(convenzione di Strasburgo) e la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU).

La protezione dei dati personali assume rilevanza innanzitutto, come diritto fondamentale della persona che nel contesto europeo è stato positivizzato nella Carta dei diritti fondamentali dell'Unione Europea e nella Convenzione Europea dei diritti dell'uomo[17].

Nella Carta il diritto alla vita privata e familiare e la tutela della protezione dei dati sono disciplinati rispettivamente dagli articoli 7 ed 8, mentre l'articolo 8 della CEDU ricomprende la protezione dei dati nel diritto al rispetto della vita privata e familiare[18].

La Carta oggi fa parte del Trattato di Lisbona, il quale le conferisce valore di Trattato e la fa diventare pienamente vincolante per le istituzioni europee e per gli Stati membri.

La Carta di Nizza, oltre a prevedere l'inviolabilità della dignità umana, della libertà, dell'uguaglianza e della solidarietà, sancisce anche il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni (art.7) e il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano (art. 8)[19].

L'articolo 8 della Carta[20], rappresenta il punto di arrivo di un processo di codificazione e costituzionalizzazione del diritto europeo alla privacy e al tempo stesso oggi costituisce la pietra angolare del nuovo impianto normativo di cui l'Unione si è dotata . Con l'art. 8 della Carta tale diritto, da una dimensione di carattere negativo approda a una dimensione di carattere positivo, che si traduce nella tutela dei dati personali mediante la creazione di un insieme di regole e principi. Questa norma, dunque, consente di costruire un sistema di controlli e contrappesi che va oltre il concetto di consenso e che permette il

[17] A. FRANCHINA, *Spunti di riflessione sul delitto di illecito trattamento di dati personali: reato istantaneo o permanente?* in Giurisprudenza Penale Web, 2020, p. 3.

[18] S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in Rivista Italiana di diritto pubblico comunitario, 2015, p. 822.

[19]https://protezionedatipersonali.it/carta-diritti-unione-europea#:~:text=La%20Carta%20dei%20diritti%20dell,europee%20e%20gli%20Stati%20membri

[20] O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdfUE*, in (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, Carta dei diritti fondamentali dell'Unione europea, Giuffrè, 2017, pp.135, 136.

trattamento lecito dei dati, talvolta anche prescindendo da un'autorizzazione esplicita dell'interessato.

I paragrafi 2 e 3 dell'articolo 8 della Carta tendono a precisare che tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e, infine, che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente[21].

Tali prescrizioni, mutuate dagli articoli 6, 7, 12, 14 e 28 della direttiva 95/46/CE, sono parimenti codificate nel nuovo Regolamento (UE) n. 679/2016.

L'art. 8, a partire dall'entrata in vigore del Trattato di Lisbona, ma, in verità, già dalla prima proclamazione della Carta, diviene per la Corte di giustizia il vero parametro di legittimità degli atti adottati dall'Unione e dagli Stati membri, essendo oggi da respingere, anche per la presenza dell'art. 16 del TFUE come base giuridica degli atti di diritto derivato adottati in materia e, dunque, espressione di una nuova competenza dell'Unione europea, l'idea che la protezione dei dati personali da parte del diritto UE sussista solo in presenza di un legame con le libertà fondamentali sancite dai Trattati.

Anzi, l'art. 16 del TFUE, avendo introdotto nell'ordinamento giuridico dell'Unione europea una nuova e generale competenza, consente, nel rispetto dell'articolo 51 della Carta, l'applicazione dell'art. 8 della Carta ogni qual volta vengano in rilievo i dati personali, con la sola eccezione dei casi in cui si esuli dal campo di applicazione del diritto UE ovvero si versi in situazioni che ricadono sotto la competenza esclusiva degli Stati membri.

Il Trattato di Lisbona, in sostanza, può vantare il pregio di avere creato una perfetta contiguità[22] fra la Carta e i Trattati, determinando una chiara ripartizione funzionale delle due norme evocate cosicché l'art. 16 del TFUE viene richiamato dal legislatore come base giuridica degli atti di rango secondario adottati in materia, mentre l'art. 8 della Carta, nella

[21] Sentenza 9 marzo 2017, Manni, C-398/15, EU:C:2017:19

[22] F. BALDUCCI ROMANO, *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia*, in Rivista italiana di diritto pubblico comunitario, 2015, p. 1658.

lettura che di tale norma dà la Corte, sovviene laddove quei medesimi atti o disposizioni di diritto interno comprimano le tutele di questo nuovo diritto fondamentale, con l'ulteriore conseguenza di rendere di fatto pacifica l'efficacia orizzontale dell'art. 8 per osmosi e, dunque, la sua applicazione nelle controversie fra privati[23] .

In una società caratterizzata da un avanzato processo di globalizzazione e da rapidi cambiamenti tecnologici, è necessario rafforzare la posizione dell'UE in rapporto alla protezione dei dati personali in tutte le politiche dell'Unione, compreso il contrasto e la prevenzione della criminalità e nelle relazioni internazionali.

L'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950 sancisce il diritto di ogni persona al rispetto della propria vita privata e familiare, del domicilio e della corrispondenza. La disposizione contenuta nell'art.8 infatti prevede che:

«1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

L'art. 7 della Carta, invece, con formulazione più schematica, dispone che: «*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*».

Il diritto al rispetto della vita privata ha trovato attuazione nell'ordinamento giuridico dell'Unione europea attraverso una serie di principi e di norme di diritto derivato che, ancorché non menzionino espressamente tale diritto, sono state interpretate dalla Corte di giustizia nel senso che tale diritto debba essere preso in adeguata considerazione e ad esso debba essere accordata adeguata tutela.

[23] O. POLLICINO*, L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in Rivista diritto dei media, 2018, p. 1.

Per comprendere il significato del rispetto della vita privata, infatti, basta considerare come tale principio abbia trovato riconoscimento nella comunità internazionale e nelle diverse fonti di diritto internazionale di origine convenzionale, che lo ricomprendono tra i diritti fondamentali.

L'art. 8 della CEDU e l'art. 7 della Carta costituiscono la riaffermazione e l'evoluzione di un principio già sancito nell'ambito dell'Organizzazione delle Nazioni Unite, dall'art. 12 della Dichiarazione universale dei diritti umani: «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni»[24].

Insomma, nella Carta il diritto alla vita privata e familiare e la tutela della protezione dei dati sono disciplinati rispettivamente dagli articoli 7 ed 8, mentre l'articolo 8 della CEDU ricomprende la protezione dei dati nel diritto al rispetto della vita privata e familiare[25]. Sicuramente tutto ciò va interpretato alla luce della diversa epoca in cui tali diritti sono stati consacrati e nei quasi cinquant'anni che separano l'adozione della CEDU dalla proclamazione della Carta di Nizza.

Analizziamo ora l'art. 52, par. 1 della Carta secondo cui «*eventuali limitazioni all'esercizio dei diritti e delle libertà […] devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*»[26].

[24] La dichiarazione universale dei diritti umani è un documento sui diritti della persona, adottato dall'Assemblea generale delle Nazioni Unite nella sua terza sessione, il 10 dicembre 1948 a Parigi con la risoluzione 219077A., con 48 voti a favore e otto astensioni: Arabia Saudita, Cecoslovacchia, Iugoslavia, Polonia, Repubblica del Sudafrica, Ucraina, Unione Sovietica.

[25] S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, op.cit.

[26] F. FERRARO, N. LAZZERINI, *Commento all'art. 52 CdfUE*, (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, Carta dei diritti fondamentali dell'Unione europea, 2017, p. 1061.

Nel dare applicazione a questa norma, la Corte verifica, in primis, se la limitazione del diritto alla protezione dei dati personali sia prevista dalla legge che, secondo la dottrina della c.d. "qualità della legge" elaborata dalla Corte EDU, deve essere sufficientemente chiara e prevedibile[27] per quanto riguarda il significato e la natura delle misure applicabili, poiché deve consentire al cittadino di immaginare le conseguenze causate dal proprio comportamento.

Inoltre, è necessario valutare se la norma limitativa del diritto persegua una finalità legittima come ad esempio, la tutela dell'ordine pubblico, la lotta alla criminalità o una azione di prevenzione dei reati, causando diversamente, il rischio di una compressione o limitazione del diritto che viene in rilievo[28] .

In terzo luogo, si deve verificare se la limitazione apportata al diritto ne possa pregiudicare il contenuto essenziale[29], sia idonea a realizzare l'obiettivo e non vada oltre il necessario per conseguirlo e, quindi, non violi i principi di proporzionalità e necessità[30] . Numerose sono, a tal proposito, le pronunce in cui la Corte si è soffermata sul rapporto fra la protezione dei dati personali, la libertà di espressione e i diritti economici degli operatori. Possiamo citare, ad esempio, le sentenze Satamedia , Scarlet , SABAM e Lindqvist [31].

La protezione dei dati personali è andata via via assumendo nell'ordinamento internazionale ed in quello dei singoli Stati una rilevanza autonoma con la previsione di apposite disposizioni ad essa dedicate dalle più recenti fonti normative.

Il trattato sul funzionamento dell'Unione europea (TFUE), modificato dall'articolo 2 del trattato di Lisbona del 13 dicembre 2007 e ratificato dall'Italia con legge 2 agosto 2008,

[27] Sentenza del 3 luglio 2007, Tan c. Turchia, ricorso 9460/03. 54 Sentenza del 24 aprile 1990, Kruslin c. Francia, ric. 11801/85, e del 25 settembre 2006, Coban c. Spagna, ric. 17060/02.

[28] Sentenza del 16 dicembre 2008, Huber, C-524/06, EU:C:2008:724, punto 69 ss.

[29] Sentenza dell'8 aprile 2014, Digital Rights Ireland Ltd, C-293/12 e C-594/12, EU:C:2014:238, punto 39.

[30] Sentenza del 9 novembre 2010, Volker und Markus Schecke e Eifert, cit., punto 52. Per la Corte, le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondono a quelle tollerate nell'ambito dell'art. 8 della CEDU

[31] Sentenza del 16 dicembre 2008, Satamedia, C-73/07, EU:C:2008:727; Sentenza del 24 novembre 2011, Scarlet, C-70/10; Sentenza del 16 febbraio 2012, SABAM, C-360/10, EU:C:2012:85; Sentenza del 6 novembre 2003, Lindqvist, C-101/01.

n. 130, rappresenta insieme al trattato sull'Unione europea (TUE), uno dei Trattati fondamentali.

Il TUE o Trattato di Maastricht è entrato in vigore nel 1993. Il TFUE, invece, l'ex Trattato che istituisce la Comunità Economica Europea, è entrato in vigore nel 1958, il cui nome è variato una prima volta con l'entrata in vigore del TUE nel 1993 e una seconda (e finora ultima) volta con l'entrata in vigore del Trattato di Lisbona nel dicembre 2009, acquisendo l'attuale definizione (TFUE). Il Trattato di Lisbona rinvia ad entrambi[32].

Prima dell'entrata in vigore del trattato di Lisbona, la legislazione in materia di protezione dei dati personali nello spazio di libertà, sicurezza e giustizia era divisa tra il primo pilastro (protezione dei dati a fini privati e commerciali, soggetta al metodo comunitario) e il terzo pilastro (protezione dei dati per scopi di ordine pubblico, con decisioni prese a livello intergovernativo). Di conseguenza, il processo decisionale seguiva due insiemi di norme.

La struttura a pilastri è venuta meno con il trattato di Lisbona, che fornisce una base più solida per lo sviluppo di un sistema di protezione dei dati più chiaro ed efficace, conferendo al contempo nuovi poteri al Parlamento europeo, che assume così il ruolo di co-legislatore.

In base all'articolo 16 TFUE, il Parlamento e il Consiglio stabiliscono le norme riguardanti la protezione delle persone fisiche in riferimento al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e delle agenzie dell'Unione, nonché da parte degli Stati membri, nell'esercizio di quelle attività che rientrano nel campo di applicazione del diritto della UE.

In seguito al programma di Tampere (ottobre 1999) e al programma dell'Aia (novembre 2004), nel dicembre 2009 il Consiglio europeo ha approvato, invece, il nuovo

[32] Il Trattato di Lisbona aumenta i poteri del Parlamento europeo e prevede diverse novità per adeguare le Istituzioni europee all'allargamento dell'UE, modifica il trattato sull'Unione europea (TUE) e il trattato che istituisce la Comunità europea, ha altresì modificato il funzionamento delle Istituzioni europee e il processo decisionale. (GU C 306 del 17.12.2007).

programma pluriennale per lo spazio di libertà, sicurezza e giustizia per il periodo 2010-2014, conosciuto come programma di Stoccolma[33].

Dunque, possiamo affermare che, nonostante venga generalmente considerato come ricompreso nel diritto al rispetto della vita privata, il diritto dell'Unione europea dedica al diritto alla tutela dei dati personali disposizioni specifiche.

La base giuridica è pertanto costituita da:

- Articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE);
- Articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea[34].

L'art. 8 della Carta fa da pendant all'art. 16 TFUE, che dispone testualmente che: "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". La medesima disposizione stabilisce che l'attuazione di tale principio per quanto attiene al trattamento e alla libera circolazione dei dati personali dovrà essere declinata e garantita attraverso l'adozione di atti di diritto derivato contenenti norme rivolte sia alle istituzioni, agli organi e agli organismi dell'Unione, sia agli Stati membri, demandando il compito di vigilare sul loro rispetto al controllo di autorità indipendenti. La Corte di Giustizia ha poi avuto più volte occasione di pronunciarsi su diversi aspetti connessi alla tutela dei dati personali definendo l'interpretazione e la portata del contesto normativo applicabile alla tutela dei dati personali[35]. Fra le sentenze più recenti e significative in materia si rammentano, in particolare, quella in cui la Corte ha affermato come la tutela dei dati personali possa legittimamente essere invocata come limite all'esercizio del diritto di accesso agli atti [36] ma anche quella che ha riconosciuto il c.d. diritto all'oblio stabilendo che

[33] Il programma di Stoccolma in materia di libertà, sicurezza e giustizia. Il programma pluriennale per lo Spazio di libertà, sicurezza e giustizia per il periodo 2010-2014 (programma di Stoccolma), che segue il programma dell'Aia (2004-2009), è stato adottato dal Consiglio europeo del 10 e 11 dicembre 2009.

[34]https://www.europarl.europa.eu/factsheets/it/sheet/157/protezione-dei-dati-personali.*Note tematiche sull'Unione europea*

[35] Per un approfondimento sulla giurisprudenza evolutiva della Corte di giustizia in materia di dati personali, G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in Studi sull'integrazione europea, 2018, p. 9; F. BALDUCCI ROMANO, Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia, op.cit. p. 1619.

[36] Cort. giust., 29 giugno 2010, causa C-28/08 P, Bavarian Lager, ECLI:EU:C:2010:378. La Corte aveva ritenuto legittima la condotta della Commissione che nel rilasciare al richiedente il verbale di

si può chiedere la rimozione di un risultato della ricerca su Google, se il contenuto è "non più rilevante"[37].

Un'altra sentenza definisce dati personali le informazioni riportate in un registro dell'orario di lavoro che contiene l'indicazione dell'ora in cui ciascun lavoratore inizia e termina l'attività lavorativa, nonché delle relative interruzioni e pause.[38]

Infine la sentenza Schrems,[39] relativa alla legittimità del trasferimento dei dati personali al di fuori dell'Unione europea [40]. Le sentenze si rifanno alla normativa europea che afferma che uno Stato membro dell'Unione Europea può verificare la richiesta di garanzia di protezione, fatta da una persona, riguardo alla tutela dei suoi dati personali, nel caso questi vengano trasferiti da uno Stato membro verso un paese terzo e non venga garantito un livello di protezione almeno equivalente.

Il quadro normativo muta radicalmente con l'adozione del regolamento 2016/679 definito con l'acronimo inglese GDPR[41]. Il regolamento, come vedremo più avanti, non solo introduce una disciplina armonizzata a fronte delle disposizioni contenute nella direttiva 95/46/CE (che viene contestualmente abrogata), che si limitava a coordinare le

una riunione svolta nell'ambito di un procedimento di infrazione ex art. 258 TFUE aveva espunto i nominativi dei partecipanti che non avevano fornito il consenso alla divulgazione della loro identità. Viene così affermato il principio che quando la richiesta di accesso riguarda documenti che comprendono anche dati personali il richiedente deve dimostrare la necessità di tale divulgazione ai sensi dell'art. 8 del regolamento 45/2001.

[37] Cort. giust., 13 maggio 2014, causa C-131/12, Google Spain, ECLI:EU:C:2014:317. La Corte si è definitivamente pronunciata, in tema di diritto all'oblio su Google, nell'ambito della causa vertente tra Google Spain e Google Inc., da una parte, e Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, dall'altra. Il gestore di un motore di ricerca su Internet è responsabile del trattamento da esso effettuato dei dati personali che appaiono su pagine web pubblicate da terzi.

[38] Cort. giust., 30 maggio 2013, causa C-342/12, Worten, ECLI:EU:C:2013:355.

[39] Cort. giust., 6 ottobre 2015, causa C-362/14, Schrems, ECLI:EU:C:2015:650.

[40] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA E V. ZENO-ZENCOVICH (a cura di), La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy Shield", Roma, 2016, p. 7 ss.

[41] Regolamento (UE) n. 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 (regolamento generale sulla protezione dei dati), in GUUE del 4 maggio 2016, L 119/1. Conformemente a quanto previsto dall'art. 99(2), il regolamento è divenuto applicabile a decorrere dal 25 maggio 2018.

diverse disposizioni nazionali vigenti, ma rappresenta un radicale mutamento di approccio rispetto al tema della tutela dei dati personali e del rispetto della vita privata.

Viene introdotto un articolato sistema di controlli e di responsabilità in capo a coloro che intervengono nei processi di trattamento, siano essi titolari (data controller) o responsabili (data processor).

Viene ampliato inoltre il sistema di garanzie a tutela dell'individuo, limitando il potere di ingerenza nella sua vita privata alle ipotesi previste dalla legge ovvero, ai casi in cui venga dimostrato un interesse pubblico superiore.

Le disposizioni dell'articolo 8 della Carta concernenti il principio del trattamento dei dati personali basato sul consenso della persona interessata nonché sul principio di lealtà e per finalità determinate sono codificate nel GDPR, che ha inoltre cristallizzato l'acquis communautaire concernente la protezione dei dati personali[42]. Dalla legge 675 del 1996 tutto è cambiato. Tabula rasa o se si preferisce, click sul tasto reset e si ricomincia da capo: sia dal punto di vista normativo sia da un punto di vista socio-tecnologico[43].

Prima che la diffusione di nuove tecnologie permettesse di raccogliere, organizzare e trasmettere una serie indistinta di informazioni personali in modo velocissimo e per finalità più differenti – il diritto alla privacy coincideva con il *the right to be let alone* di memoria statunitense, il quale riconosceva all'individuo il diritto di essere lasciato solo, in pace, indisturbato; di godere, così, di una sfera riservata e intima al riparo dall'altrui intrusione e sguardo indiscreto.

Storicamente il diritto alla privacy, inteso, dal punto di vista giuridico, infatti, nacque proprio con la famosa espressione "the right to be let alone"[44] coniata nel 1890, all'interno

[42] F. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679*, in Eurojus, 2018, pp. 5-6, http://rivista.eurojus.it/alcuneriflessioni-a-margine-della-nuova-disciplina-in-materia-di-protezione-dei-dati-personali-di-cui-al-regolamentoue-2016679ue/.

[43] A. CICCIA MESSINA, *Guida al codice privacy. Come cambia dopo il GDPR e il D.Lgs. n.101/2018*, Wolters Kluwer, Milano, 2019, Prefazione, p. IX

[44] S. RODOTÀ, *Intervista su privacy e libertà*, a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005, p. 8.

del saggio The Right to Privacy[45] di Brandeis e Warren,che ebbe il merito di avviare una vera e propria rivoluzione giuridica e sistematica sul concetto di privacy. Il saggio nacque a seguito di una vicenda strettamente personale riguardante la vita matrimoniale dello stesso Warren. Sono passati oltre cent'anni dalla pubblicazione dell'articolo[46], pietra angolare su cui poggia il moderno istituto giuridico della privacy, in cui i due studiosi americani si ritrovarono a riflettere su quali informazioni riguardanti la vita personale di un individuo dovessero essere di pubblico dominio e quali, invece, meritassero di essere preservati dall'invadenza altrui.

Guardando a invenzioni e tecniche commerciali di allora come la stampa a rotativa, veloce sistema di diffusione delle notizie, Brandeis e Warren iniziarono ad interessarsi ad una serie di casi in cui le invenzioni del loro tempo, compresa la fotografia, potevano dar luogo a tutta una serie di violazioni della riservatezza dell'individuo, divulgando dettagli e particolari sulla vita privata di ognuno.

Il loro saggio, The right of privacy, ebbe il merito di avviare una sistematica discussione sul concetto di privacy invocando l'adozione di misure da intraprendere per la tutela della persona.

Dopo un lungo e travagliato processo di riconoscimento e di affermazione, l'iniziale diritto ad essere lasciati soli si è trasformato, quindi, nel diritto alla protezione dei dati personali il quale oramai assurge a diritto fondamentale della persona sia all'interno del sistema giuridico nazionale che nell'alveo di quello comunitario.

[45] L.D. BRANDEIS, S. WARREN, *The Right to Privacy*, in 4 Harward Law Review, 1890, pp. 193- 220.

[46] V. SALVATORE *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato, op.cit.*

1.2. Dal Codice Privacy al GDPR

In Italia, la prima legge che organicamente si occupa del trattamento dei dati personali è, come noto, la legge n. 675/1996[47] "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", il cui art. 1 stabilisce che «la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale».

A questa statuizione si ricollegava chiaramente l'istituzione del "`Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" (art. 30, 1° co.). In realtà, pochi mesi dopo questa disposizione veniva modificata, prevedendosi l'istituzione del Garante per la protezione dei dati personali[48].

Si può pertanto osservare che è "per via istituzionale"' che fa (pieno) ingresso nel nostro ordinamento positivo il riferimento alla protezione dei dati personali e, seppure implicitamente, una situazione soggettiva che a quella protezione, garantita da una autorità pubblica, faccia riferimento[49].

È con il codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) che si consolida normativamente questa dimensione della tutela dei dati personali. L'art. 1 del codice afferma che «*chiunque ha diritto alla protezione dei dati personali che lo riguardano*» mentre l'art. 2 amplia, in sostanza, le finalità del codice alla garanzia *«che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*».

Rispetto a quanto previsto nella l. 675/1996, fa il suo ingresso nel codice il diritto alla protezione dei dati personali. Questo diritto, sul piano delle finalità connesse con la sua tutela, si affianca alla riservatezza ed alla identità personale.

Si possono quindi sintetizzare due aspetti.

[47] Legge 31 dicembre 1996, n. 675, pubblicata nella Gazzetta Ufficiale n. 5 dell'8 gennaio 1997.

[48] Art.3, 1° co., d.lgs. n. 123/1997.

[49] In base a quanto indicato dall'art. 28, Direttiva 95/46CE.

A quanto risulta, solo nel 1997, in Italia, si ha una prima formalizzazione legislativa del concetto di protezione dei dati personali, attraverso la qualificazione dell'attività di una autorità indipendente.

Nel 2003 quel concetto viene canonizzato come diritto appartenente a chiunque, finalizzato a garantire una molteplicità di diritti come quello alla riservatezza e alla identità personale, all'interno di un più generico riferimento a dignità, diritti e libertà fondamentali dell'interessato.

Queste osservazioni spiegano molto della impostazione della dottrina italiana e dello stretto legame (che diviene talvolta sovrapposizione) tra i concetti di riservatezza, da un lato, e protezione dei dati personali, dall'altro.

In Italia, nel secondo dopoguerra, si è progressivamente e faticosamente fatto strada il diritto alla riservatezza[50] e alla tutela della vita privata[51], inteso come traslazione del diritto di essere lasciato da solo, del diritto alla privacy nella accezione originariamente affermatasi negli Stati Uniti. Questo diritto si è alla fine affermato per via giurisprudenziale, grazie ad una famosa sentenza della Cassazione civile del 1975, nel caso Soraya.

Deve essere rilevato che pressoché tutta la capillare normativa che - nei più diversi settori e ambiti giuridici - oggi si riconosce unanimemente svolgere una funzione di tutela della riservatezza, in realtà è stata adottata prima che un formale riconoscimento (giurisprudenziale) della riservatezza come diritto avesse luogo (si pensi alle disposizioni, di assoluto rilievo, dello Statuto dei lavoratori del 1970) e, comunque, anche successivamente, a prescindere da una puntuale consapevolezza dell'esistenza e del perimetro di un tale diritto: si tratta di disposizioni disseminate nell'ordinamento, «senza trovare un reale momento di unificazione»[52].

[50] A. DE CUPIS, *Il diritto alla riservatezza esiste*, in Foro it., IV, 1954, p.90 ss.

[51] F. CARNELUTTI, *Diritto alla vita privata*, Riv. trim. dir. pubbl., 1955, p.3 ss.

[52] R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in Diritto alla riservatezza e circolazione dei dati personali, a cura di Pardolesi, Milano, 2003, p.17.

Questo aspetto è particolarmente rilevante, poiché, mentre pian piano si affermava in Italia la dimensione della riservatezza, l'originario concetto di privacy si veniva modificando e allargando, sia negli Stati Uniti, sia nei paesi europei più avanzati[53].

Recenti approfondimenti dottrinali hanno messo in luce questa progressiva metamorfosi della nozione della privacy e le sue problematiche semantiche, ma il primo aspetto da sottolineare è che in ambito europeo diversi Stati (e la stessa Comunità economica europea) cominciano ad avvedersi che l'avvento dell'informatica produce una nuova dimensione del problema della privacy[54], che a partire dagli anni Settanta conduce alla progressiva introduzione di leggi volte alla protezione dei dati personali.

Questi corpi normativi hanno l'effetto di muovere non solo il dibattito dottrinale, ma principalmente gli assetti istituzionali - nascono le prime autorità indipendenti di settore, ad es. in Germania[55] - e la coscienza socio-economica dei paesi interessati sul rilievo giuridico della nuova dimensione della privacy. Come si vedrà non è un caso che l'approfondita elaborazione della giurisprudenza costituzionale tedesca del diritto all'autodeterminazione informativa risalga agli anni Ottanta, mentre (- inevitabilmente -) nel nostro ordinamento ancora si discuteva di riservatezza e vita privata.

In qualche modo, pertanto, riservatezza e protezione dei dati personali risultano, in Italia, nozioni *storicamente* sovrapposte e non è raro osservare che la protezione dei dati venga ritenuta una nuova dimensione della riservatezza, la quale a sua volta è intesa come sinonimo di privacy, nelle diverse accezioni assunte dal concetto.

Solo in concomitanza con l'approvazione della legge n. 675/1996 e del d.lgs. n. 196/2003[56], si è potuto intraprendere un faticoso lavoro di distinzione del diritto alla riservatezza dal diritto alla protezione dei dati personali[57].

---

[53] A. CERRI, *Riservatezza (diritto alla*), II, Diritto comparato e straniero», in Enc. giur., Roma, 1991.

[54] G. RESTA, *Il diritto alla protezione dei dati personali*, in CARDARELLI-SICA-ZENO ZENCOVICH, *Il codice dei dati personali*, Milano, 2003, p.32 ss.

[55] M.G. LOSANO, *La legislazione tedesca sulla protezione dei dati individuali*, in ALPA-BESSONE, *Banche dati telematica e diritti della persona*, Padova, 1984, p.279, p.285.

[56] DECRETO LEGISLATIVO 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, *recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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*.

Di recente, si afferma consapevolmente che «*il diritto alla protezione dei dati personali assume la connotazione di un nuovo diritto in grado di garantire a chiunque una piena scelta sul destino dei propri dati personali: e, quindi, non più il mero arroccamento su di sé, l'isolamento dalla comunità, ma al contrario la libertà di condividere entro limiti ragionevoli*». Si tratta di un «*nuovo diritto all'autodeterminazione informativa, in grado di tutelare i flussi informativi connessi ai dati personali in ogni settore pubblico e privato, estendendo o comunque declinando in termini più ampi il concetto di riservatezza*»[58].

In questo contesto, pur se a tratti inevitabilmente connesse e sovrapposte, riservatezza e protezione dei dati personali risultano distinguibili, sulla linea di confine fra libertà negativa (diritto di escludere) e libertà intrinsecamente positiva (diritto di controllare, autodeterminazione informativa) ed a loro volta si distinguono dal diritto all'identità personale (come «diritto a non vedere travisata la propria immagine sociale»): si tratta delle facce di un unico prisma, legato alla personalità umana.

Caratteristica peculiare della disciplina della protezione dei dati italiana è dunque di essere sopraggiunta solo alla fine degli anni Novanta, quando un insieme di fattori ne rendevano ineludibile l'approvazione.

In primo luogo, sulla scia della previsione dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (Cedu) del 1950, il Consiglio d'Europa già nel 1981 aveva promosso la sottoscrizione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (n. 108/1981), la quale impegnava gli Stati aderenti ad adottare «nel proprio diritto interno, le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati» (art. 4, 1° co.).

Inoltre, l'Unione europea aveva adottato la direttiva 95/46CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che doveva essere attuata a livello nazionale.

Per queste ragioni, viene approvata la legge n. 675/1996 e, nel volgere di qualche anno, per dare completa attuazione anche alla direttiva 2002/58/CE relativa al trattamento

[57] D. VANNI, *Protezione dei dati personali* (dir. civ.)», in *Digesto/civ.*, *Agg*., Torino, 2013.

[58] L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, p.15.

dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, viene approvato il d.lgs. n. 196/2003, recante un ben più corposo e comprensivo "codice in materia di protezione dei dati personali".

Il codice si caratterizza per una spiccata vocazione ordinamentale[59].

Il codice aveva ed ha la pretesa di disciplinare in modo organico sia gli aspetti sostanziali della materia, sia i profili istituzionali, sia le modalità evolutive di implementazione della disciplina di protezione dei dati personali nei diversi settori rilevanti, sia i profili concernenti il livello rimediale e sanzionatorio. Complessivamente, il codice rappresenta l'ordinamento della protezione dei dati personali in Italia. Questo profilo marca la principale distinzione, sul piano normativo, fra la riservatezza[60] e la protezione dei dati personali.

In quest'ultimo caso, quando si discute - come si è fatto in precedenza - del diritto alla protezione dei dati personali come di una libertà 'attiva' è opportuno specificare che si tratta di una libertà presidiata da un quadro normativo omogeneo e da istituzioni dedicate[61].

Di fondamentale stimolo per l'adozione della nuova normativa è risultata la necessità per il nostro Paese di dare adempimento ad obblighi assunti sul piano internazionale ed in ambito comunitario.

Vengono in rilievo, in particolare, due testi normativi.

In primo luogo, la Convenzione del Consiglio d'Europa n. 108/1981. in riferimento a quest'ultima possiamo affermare che anche l'Italia, come hanno fatto nel corso degli anni tutti gli altri Paesi dell'Unione europea, aveva deciso di aderire alla Convenzione, con la legge 21-2-1989, n. 98, che ne ha autorizzato la ratifica. Ma, fino all'emanazione della legge n. 675/1996, la ratifica non aveva potuto essere formalizzata, essendo il nostro

[59] M. CARTABIA, *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto,* in LOSANO (a cura di), La legge italiana sulla privacy. Un bilancio dei primi cinque anni, Roma-Bari, 2001, p.59 ss. (spec. 61-62).

[60] G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza, in I diritti costituzionali*, R. Nania, P. Ridola (a cura di), vol. 2, Torino, Giappichelli, 2006, p. 627.

[61] A. BARBERA, *Art. 2 Costituzione*, in Principi fondamentali (artt. 1-12), Commentario della Costituzione, *G.* Branca (a cura di), Zanichelli Editore, Bologna-Roma, 1975.

Paese inadempiente all'obbligo previsto dall'art. 4 della Convenzione di adottare, nel proprio diritto interno, «le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati» enunciati in tale atto[62].

In secondo luogo, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24-10-1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Di questa la legge n. 675 costituisce tempestiva attuazione. L'Italia è il primo Paese ad avere dato attuazione alla direttiva, attraverso l'emanazione di una normativa organica, molto articolata, utilizzando i margini di manovra, talvolta anche ampi, che la direttiva stessa riconosce ai legislatori nazionali (cfr. il «considerando» n. 9). Per gli altri Stati membri, si porrà, piuttosto, un problema di verifica della compatibilità, ed eventualmente di adattamento alla direttiva, della normativa nazionale preesistente[63].

Possiamo affermare, dunque, che la Convenzione n. 108 rappresenta il risultato finale di un percorso graduale di analisi, seguito dal Consiglio d'Europa del problema della tutela della riservatezza a fronte dell'evoluzione e della diffusione delle tecniche informatiche di raccolta e trattamento delle informazioni, tanto nel settore pubblico quanto in quello privato, analisi scandita da alcune risoluzioni adottate (Risoluzione 26-9-1973[64] 20-9-1974[65]). Alla base di questi atti, in rispondenza degli scopi propri del Consiglio d'Europa, era affermata l'esigenza di rafforzare la tutela dei diritti umani e delle libertà fondamentali, in particolare di quelli previsti espressamente dagli articoli 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[66].

Dalle indicazioni fornite agli Stati membri per invitarli ad attenuare le divergenze

[62] Lo strumento di ratifica è stato depositato il 29-3-1997 e la Convenzione è entrata in vigore in Italia il 1-7-1997.

[63] E. CANNIZZARO, *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Seconda edizione, Torino, Giappichelli, 2017, p. 115 ss.

[64] 64 Risoluzione del Consiglio d'Europa sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato. Adottata dal Comitato dei Ministri il 26 settembre 1973 durante la 224ma riunione dei Delegati dei Ministri.

[65] 65 Risoluzione del Consiglio d'Europa sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico. Adottata dal Comitato dei Ministri il 20 settembre 1974 durante la 236ma riunione dei Delegati dei Ministri.

[66] G. BUTTARELLI, *Banche dati e tutela alla riservatezza*, Giuffrè. Milano, 1997, p. 296 ss.

esistenti fra i rispettivi ordinamenti, si passava, nelle Risoluzioni, a prefigurare le linee fondamentali alle quali si sarebbe dovuta ispirare una Convenzione che veniva individuata come lo strumento più idoneo per assicurare un livello minimo comune di garanzie per le persone nel territorio di ciascuna Parte aderente.

Si realizzava così in quegli anni un proficuo processo di circolazione di principi e modelli di disciplina della «privacy informatica»: queste risoluzioni, infatti, da un lato, offrivano delle indicazioni ai legislatori dei Paesi nei quali, in quel periodo, venivano emanate le prime normative organiche in materia, dall'altro, valutavano e rielaboravano le esperienze che andavano maturando a livello nazionale.

Nel 1981, infine, veniva adottata la già ricordata Convenzione n. 108, il cui progetto era stato elaborato in stretto raccordo con la Commissione delle Comunità europee e con l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE).

Merita accennare come anche quest'ultima organizzazione, l'OCSE, avesse negli anni Settanta dedicato grande attenzione al tema della disciplina del trattamento dei dati, quale strumento per favorire, attraverso la libera circolazione delle informazioni fra gli Stati membri, la politica di integrazione economica da essa perseguita. L'atto che in maniera più significativa esprime tale attenzione è la raccomandazione del 23-9-1980[67], concernente le linee direttive riguardanti la protezione della vita privata e la circolazione transnazionale dei dati a carattere personale. Questo documento, privo di efficacia vincolante per i Paesi membri, anticipava i principi che poi sarebbero stati affermati nella Convenzione del Consiglio d'Europa dell'anno successivo.

La Convenzione n. 108 riguarda la sola elaborazione automatizzata di dati di carattere personale, compiuta nei settori pubblico e privato, limitatamente alla tutela delle persone fisiche (per quanto gli Stati possano estenderne l'applicazione alle persone giuridiche ed agli enti di fatto).

In essa vengono fissati alcuni principi fondamentali ai quali le Parti devono conformare la propria legislazione interna (la Convenzione non è infatti, in linea di principio, self-executing), per consentire il raggiungimento di un livello minimo di protezione uniforme che favorisca la libera circolazione dei dati. Si tratta di almeno sei

[67] Linee-guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali, del 23 settembre 1980 [C(80)58(Final).

principi, che è bene qui richiamare. Innanzitutto il principio ‘della qualità dei dati raccolti’. Si sostanzia nella correttezza e liceità dell'attività di raccolta ed elaborazione dei dati e nella esattezza ed aggiornamento di questi ultimi (art. 5). Segue il principio ‘di finalità’, alla luce della finalità perseguita da chi tratta i dati deve essere valutata la legittimità della raccolta (che può riguardare solo i dati pertinenti) e dell'impiego dei dati (che deve avvenire in maniera non incompatibile con le finalità) e la sussistenza dell'obbligo di trasformazione delle informazioni riferite a soggetti identificati od identificabili in dati anonimi (art. 5). A questi si aggiunge il principio di ‘pubblicità’ dell'attività di trattamento delle informazioni personali (artt. 8 e 13) e il principio ‘di tutela rafforzata dei dati sensibili’, dati indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni e dati relativi allo stato di salute o alla vita sessuale. A questi la Convenzione equipara i dati relativi alle condanne penali: la Convenzione ne vieta l'elaborazione automatica a meno che il diritto interno non preveda appropriate garanzie (art. 6). Invece, il principio ‘dell'accesso individuale’ della persona alla quale i dati si riferiscono, intende esercitare il controllo sulle informazioni trattate, per ottenere la rettifica e la cancellazione dei dati elaborati in violazione delle norme sulla qualità delle informazioni e sull'impiego dei dati sensibili (art. 8). Infine, il principio della ‘sicurezza fisica e logica dei dati’, per prevenire la distruzione accidentale o non autorizzata ovvero la perdita accidentale dei dati, come pure l'accesso ai dati, la modifica o la diffusione non autorizzati (art. 7; è l'unico principio per il quale non è ammessa alcuna deroga)[68]

I principi affermati nella Convenzione n. 108 hanno poi trovato specificazione in una serie di raccomandazioni relative a determinati settori, adottate dal Consiglio d'Europa a partire dal 1981. Vengono presi in considerazione i trattamenti di dati effettuati nell'ambito di attività o da soggetti particolari, rispetto ai quali maggiori appaiono i rischi di invasione della sfera privata, per la natura dei dati trattati o per l'ampio e pervasivo impiego di strumenti informatici e telematici (la prima di queste raccomandazioni, riguardante i dati sanitari, è del 1981). Alcune raccomandazioni hanno assunto un particolare rilievo nel nostro ordinamento, essendo divenute vincolanti per il legislatore. Come meglio vedremo

[68] Secondo l'art. 9 della Convenzione è possibile invece che ciascuno Stato aderente deroghi agli altri principi per la protezione dei dati, quando la deroga sia prevista dalla legge e costituisca una misura necessaria in una società democratica per la tutela di determinati interessi collettivi o individuali.

infatti, il Governo doveva garantire la piena attuazione dei principi in esse affermati nell'emanare, sulla base della delega conferita dalla legge n. 676 del 1996, i decreti legislativi contenenti la disciplina di particolari ipotesi di trattamento dei dati.

Passando all'ambito comunitario, fra i vari interventi che hanno preceduto l'emanazione della direttiva 95/46 ci si può in questa sede limitare a richiamare due risoluzioni del Parlamento europeo, dell'8-4-1976 e dell'8-5-1979, che, da un lato, sottolineavano l'esigenza di tutela dell'individuo di fronte al progresso tecnico nel settore dell'informatica, dall'altro, evidenziavano la necessità che la Commissione predisponesse una proposta di direttiva che fosse idonea a «garantire una protezione al più alto livello per i cittadini della Comunità».

La proposta della Commissione veniva presentata nel 1990. Dopo la presentazione, nel 1992, di una proposta modificata, si giungeva all'approvazione nel 1995, dopo un iter particolarmente laborioso: il problema era quello di trovare il consenso degli Stati membri su uno standard di tutela accettabile da tutti alla luce delle normative nazionali già esistenti.

Si intendeva intervenire per eliminare le divergenze ancora presenti fra le legislazioni nazionali, suscettibili di frenare la libera circolazione delle informazioni nell'ambito del mercato interno, e per disciplinare la circolazione delle informazioni nei confronti degli Stati terzi. Il fatto che tutti gli Stati membri avessero ratificato la Convenzione n. 108 non garantiva di per sé un sufficiente grado di uniformità delle legislazioni nazionali, attesa l'ampia discrezionalità che tale atto lascia alle parti contraenti nell'adozione delle misure di implementazione dei principi in esso contenuti.

Dall'altro lato, appariva opportuno definire un nuovo quadro di riferimento per le legislazioni nazionali aggiornando e sviluppando, alla luce dell'esperienza applicativa maturata e, soprattutto, dei progressi tecnici intervenuti, i contenuti della Convenzione n. 108, pur restando fedeli alle linee di fondo che ne avevano ispirato la stesura. In maniera esplicita la direttiva 95/46 si ricollega alle iniziative del Consiglio d'Europa. Al decimo «considerando» è richiamato l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. All'undicesimo «considerando» è affermato che i principi di tutela delle persone, in particolare della vita privata, contenuti nella direttiva «precisano ed ampliano» quelli enunciati dalla Convenzione n. 108.

Come quest'ultima, la direttiva nasce con l'obiettivo di costruire un quadro normativo, quanto più possibile uniforme fra gli Stati membri, che consenta l'equilibrio fra due

contrapposte esigenze, e fra i contrapposti interessi a queste sottesi: da un lato, la tutela, con riguardo al trattamento dei dati, della libertà e dei diritti delle persone fisiche (delle persone, in termini assoluti, piuttosto che degli «utenti», o dei «consumatori» o dei «cittadini» nei loro rapporti con la pubblica amministrazione), in particolare della vita privata, dall'altro lato, la libera circolazione dei dati personali (funzionale al corretto svolgimento delle attività economiche ed all'adempimento dei compiti delle pubbliche amministrazioni)[69].

La libera circolazione dei dati è ritenuta condizione indispensabile alla effettiva realizzazione e funzionamento del mercato interno, delle libertà di circolazione delle merci, delle persone, dei servizi e dei capitali, considerando che nella Comunità si ricorre sempre più frequentemente al trattamento ed allo scambio dei dati personali, nei vari settori delle attività economiche e sociali, trattamento e scambio facilitati dai progressi fatti registrare dalle tecnologie dell'informazione.

La libera circolazione dei dati esige in primo luogo che sia assicurata la protezione dei diritti fondamentali ad un livello equivalente negli Stati membri, per non ostacolare l'esercizio di una serie di attività economiche su scala comunitaria e falsare la concorrenza, consentendo l'esistenza di «paradisi dei dati», caratterizzati da legislazioni meno garantiste, nei quali si concentrerebbe l'attività di trattamento dei dati, e lasciando spazio all'imposizione di restrizioni alla libera circolazione dei dati da parte dei singoli Stati giustificate dalla scarsa protezione accordata ai diritti della persona in altri Stati membri. Il secondo paragrafo dell'art. 1 della direttiva, su questo punto prevede che gli Stati membri, data la protezione equivalente quale si determinerà con il ravvicinamento delle legislazioni determinato dal recepimento della normativa comunitaria, non possano più restringere o vietare la libera circolazione tra loro dei dati personali per ragioni inerenti alla tutela dei diritti delle persone (cfr. il «considerando» n. 9).

Ma la direttiva persegue anche l'obiettivo di un «elevato grado di tutela nella

[69] Il rapporto fra queste due diverse prospettive risulta evidente dalla lettura del secondo «considerando» che si apre con una formula analoga a quella che apre la legge francese: «*considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà ed i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui*».

Comunità» dei diritti e delle libertà fondamentali della persona («considerando» n. 10). Quest'ultimo obiettivo, confermato dai richiami, contenuti nella parte introduttiva della direttiva, ai diritti fondamentali, «sanciti dalle costituzioni e dalle leggi degli Stati membri» (primo «considerando») e riconosciuti quali «principi generali del diritto comunitario» («considerando» n. 10), alla tutela della vita privata («considerando» n. 2 e n. 7) e alla libertà di espressione, in particolare alla libertà di ricevere o comunicare informazioni («considerando» n. 37) attribuisce alla direttiva un significato più ampio del semplice perseguimento di un obiettivo di natura esclusivamente o prettamente economica, per quanto questo sia l'obiettivo principalmente perseguito. Con questa direttiva il legislatore comunitario mostra di muoversi verso la realizzazione di un sistema giuridico nel quale trova spazio non solo la disciplina dei rapporti economici tra i soggetti, ma anche la disciplina dei diritti dell'individuo[70].

La direttiva 95/46si articola in sette capi, che si occupano di tutti i profili rilevanti della disciplina del trattamento dei dati, con riguardo a qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati su dati personali (cioè su qualsiasi informazione concernente una persona fisica, identificata o identificabile), purché tali dati siano contenuti o siano destinati a figurare in archivi strutturati secondo criteri specifici tali da facilitarne l'accesso.

Il capo I contiene le definizioni (di «dati personali», «trattamento di dati personali», «archivio», «consenso della persona interessata» e dei diversi soggetti coinvolti nel trattamento), definisce il campo di applicazione della direttiva e disciplina la normativa nazionale applicabile. Il capo II contiene le disposizioni sostanziali fondamentali della normativa, fissando le condizioni generali di liceità del trattamento dei dati. Nelle nove sezioni di cui è composto, vengono definite le regole sulla qualità dei dati, sul consenso consapevole dell'interessato e sui casi nei quali tale consenso non è necessario ai fini della legittimazione del trattamento, sul trattamento dei dati sensibili e sul trattamento dei dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, sui diritti dell'interessato, in particolare sul diritto di accesso e di opposizione al trattamento dei dati, sulla riservatezza e la sicurezza dei dati, sull'obbligo di notificazione

[70] F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in CUFFARO, RICCIUTO (a cura di), La disciplina del trattamento dei dati personali, Torino, 1997, pp. 16-17.

del trattamento all'autorità di controllo. Il capo III è costituito da tre articoli dedicati rispettivamente agli strumenti di tutela giurisdizionale, alla responsabilità per il danno cagionato da un trattamento illecito, alle sanzioni da applicare in caso di violazione delle disposizioni di attuazione della direttiva. Il capo IV disciplina il trasferimento dei dati verso Paesi terzi (terzi, ovviamente, rispetto alla Comunità). Il capo V si occupa, nell'unico articolo di cui è costituito, dei codici di condotta elaborati da associazioni professionali e da altri organismi rappresentanti determinate categorie di responsabili del trattamento. Il capo VI contiene le disposizioni relative all'istituzione delle autorità nazionali di controllo indipendenti, chiamate a verificare l'applicazione della normativa di attuazione della direttiva. Si occupa, altresì, dell'istituzione di un gruppo chiamato a svolgere attività di coordinamento delle autorità nazionali. Il capo VII, infine, riguarda le misure comunitarie di esecuzione, in particolare l'istituzione di un comitato che deve assistere la Commissione con funzioni consultive con riferimento a nuove misure da adottare in tema di privacy.

La direttiva 95/46 ha i caratteri della direttiva quadro: i principi in essa affermati sono destinati ad essere «completati o precisati, soprattutto per taluni settori, da norme specifiche ad essi conformi» («considerando» n. 68).

È quanto è accaduto nel settore delle telecomunicazioni, settore di rilievo primario, al quale le istituzioni comunitarie hanno dedicato una nutrita serie di rilevanti interventi nell'ultimo decennio, e rispetto al quale si pongono, come è evidente, notevoli problemi di data protection nella prospettiva della tutela della riservatezza. Per rispondere a questi problemi, è stata emanata la direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15-12-1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, la cui proposta era stata presentata già nel 1990 insieme alla proposta di direttiva-quadro.

La direttiva 97/66 contiene disposizioni che precisano ed integrano (art. 1, par. 2) quelle della direttiva 95/46[71], che rimane comunque applicabile anche al settore delle telecomunicazioni, in relazione agli aspetti non specificamente disciplinati dal nuovo provvedimento.

La direttiva si fa carico della tutela dei diritti delle persone fisiche, ed anche dei «legittimi interessi» delle persone giuridiche, con particolare riferimento alla fornitura di

[71] C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in Eur. dir. priv., 1998, p. 653 ss.

servizi di telecomunicazione offerti tramite la rete digitale di servizi integrati (ISDN) e le reti pubbliche digitali radiomobili (art. 3, par. 1). Si occupa, innanzitutto, della garanzia della sicurezza delle reti e della riservatezza delle comunicazioni. Definisce la disciplina del trattamento dei dati personali finalizzato alla fatturazione, alla rilevazione dei dati sul traffico ed alla produzione degli elenchi degli abbonati. Contiene disposizioni sul sistema tecnologico della *calling line identification*, sul sistema cioè che consente al soggetto che riceve la chiamata di vedere riportato su un apposito display del proprio apparecchio telefonico il numero dal quale proviene la telefonata. Si occupa, infine, delle chiamate indesiderate, in particolare di quelle a scopo pubblicitario. Anche questa direttiva, come vedremo, ha già ricevuto attuazione nell'ordinamento italiano.

1.2.1 L'evoluzione della normativa

Per chiudere questi cenni al contesto internazionale e comunitario nel quale si situa la nuova disciplina nazionale, occorre sottolineare come un'accelerazione decisiva all'iter di approvazione della legge n.675 sia derivata dalla necessità di dare piena esecuzione alla Convenzione di applicazione dell'Accordo di Schengen (la prima del 19-6-1990, il secondo del 14-6-1985), la cui ratifica è stata autorizzata in Italia con la legge 30-9-1993, n. 388.

Tale accordo, sottoscritto da tutti i Paesi membri dell'Unione europea, con eccezione di Irlanda e Regno Unito, prevede la graduale abolizione dei controlli relativi alle persone alle frontiere comuni degli Stati aderenti. Per il perseguimento di questo obiettivo è prevista la realizzazione di una rete informatica comune (Sistema di informazione Schengen), costituita da sezioni nazionali aventi sede presso i singoli Paesi aderenti (per l'Italia presso il Centro elaborazione dati del Ministero dell'interno). I Paesi membri inseriscono e traggono dal Sistema, per gli scopi propri di questo, dati relativi alle persone.

Il progredire delle decisioni della Corte di Giustizia dell'Unione europea rappresenta un osservatorio privilegiato per cogliere il percorso di avvicinamento dell'ordinamento europeo alla tutela ed alla disciplina del diritto alla protezione dei dati personali.

Nelle prime decisioni successive all'adozione della Carta, la Corte appare quasi non avvedersi dell'introduzione degli artt. 7 e 8. Si continuano a rinvenire ricorrenti riferimenti

alle finalità proprie della dir. 95/46, che vengono individuate nel mantenere un equilibrio fra la libera circolazione dei dati personali e la tutela della vita privata e nel procedere verso l'armonizzazione delle disposizioni nazionali, che, in linea di principio, dovrebbe essere completa[72]: la tutela equivalente all'interno degli Stati membri è funzionale ad una circolazione dei dati nel mercato interno.

Alcune decisioni del 2008 cominciano a spostare l'accento sulla tutela della persona e dei suoi diritti fondamentali, sancita dall'art. 1 della dir. 95/46[73], anche a causa dell'esigenza di bilanciare il diritto alla vita privata con altri diritti (segnatamente di proprietà intellettuale): nella nota sentenza Promusicae - in cui si doveva decidere se sulla base del diritto europeo vi fosse l'obbligo di comunicare dati personali di soggetti ritenuti condividere in modo illecito in rete contenuti coperti dal diritto d'autore - la Corte fa riferimento ai «diritti delineati agli artt. 7 e 8 di tale Carta», precisando che l'art. 7 «*riproduce in sostanza l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali», il quale garantisce il diritto al rispetto della vita privata, «mentre l'art. 8 della Carta proclama espressamente il diritto alla tutela dei dati personali*»[74].

Con la successiva sentenza Schecke del 2010 la Corte comincia a delineare più approfonditamente e prudentemente i caratteri del diritto alla protezione dei dati personali: sul fondamento del valore giuridico acquisito della Carta grazie all'art. 6 del TUE, si precisa che il parametro di giudizio è costituito - nella specie - dalla Carta medesima e quindi si sviluppa una descrizione articolata del contenuto e dei limiti interpretativi del diritto alla protezione dei dati personali (173). In questa decisione la Corte vuole sottolineare proprio lo stretto legame fra gli artt. 7 e 8 della Carta e l'art. 8 della Cedu (par. 52), in forza del quale «*le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle tollerate nell'ambito dell'art. 8 della CEDU*».

Con la sentenza in parola si compie pertanto un primo passaggio. Una volta entrati in vigore i nuovi Trattati, la Corte mostra di poter finalmente poggiare non più solo sulla

[72] Cort. giust. UE, 6-11-2003, causa C-101/01, Lindqvist.

[73] Cort. giust. UE, 16-12-2008, C-524/06, Heinz Huber, par. 47.

[74] Cort. Giust. UE, 29-1-2008, C-275/06, Promusicae, par. 64.

tutela (funzionale) della persona nel trattamento dei dati personali indotta dal diritto derivato, ma su un diritto fondamentale previsto dalla Carta (e dal TFUE).

Un ulteriore versante - non sempre adeguatamente sottolineato - in cui la Corte mostra di voler stabilire un punto fermo riguarda il valore riconosciuto alla proiezione istituzionale del diritto alla protezione dei dati personali: inizialmente basandosi sul solo art. 28 della dir. 95/46, poi fondandosi sull'art. 8, c. 3, della Carta ed infine aggiungendovi il riferimento all'art. 16, c. 2, TFUE, la Corte è granitica nel ritenere che l'esistenza di una autorità nazionale di controllo indipendente costituisce «un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali»[75].

Vi sono due ulteriori aspetti su cui - ai nostri fini - appare necessario volgere l'attenzione.

Il primo concerne il nesso di strumentalità che talvolta affiora fra diritto alla protezione dei dati personali e diritto alla vita privata.

In almeno tre decisioni la Corte afferma che «conformemente ad una giurisprudenza consolidata, la tutela del diritto fondamentale alla vita privata, garantito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, impone che le deroghe alla tutela dei dati personali e le limitazioni della stessa devono avvenire nei limiti dello stretto necessario»[76].

Se ci si riflette, si tratta di una statuizione che potrebbe apparire piuttosto ambigua e, invece, offre una chiave di lettura estremamente interessante e feconda sulla distinzione e, poi, sulla correlazione fra i due diritti.

La Corte afferma che per valutare la legittimità di una deroga - apparentemente plausibile, in ipotesi - alla disciplina della protezione dei dati personali in sé considerata, è necessario analizzare le ricadute che può avere sull'altro diritto, alla vita privata, poiché «occorre ricordare che la tutela dei dati personali (…) riveste un'importanza particolare per il diritto al rispetto della vita privata» (Digital Rights Ireland). In tal modo, come acutamente osservato, la Corte finisce per porre in luce che «l'art. 8 rappresenta un arricchimento della tutela del diritto fondamentale al rispetto della vita privata, anche in ragione del fatto che il diritto alla privacy e il diritto alla protezione dei dati, per quanto

[75] Cort. giust. UE, 5-5-2011, C-543/09, Deutsche Telekom AG, par. 52-53.

[76] Cort. giust. UE, 7-11-2013.

tendano a sovrapporsi, hanno due oggetti non coincidenti: il primo, uno spazio privato; il secondo, il trattamento di dati personali, indipendentemente dal fatto che siano dati privati».

Si può intuire agevolmente che il nesso strumentale fra protezione dei dati personali e vita privata è direttamente proporzionale alla evoluzione tecnologica in cui il trattamento dei dati ha luogo[77].

Facendo applicazione del principio di proporzionalità «alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta», con la sentenza Digital Rights Ireland, la Corte ha dichiarato l'invalidità della dir. 2006/24/CE (c.d. data retention)[78].

Trascorso appena un mese, con la sentenza Google Spain[79], applicando evolutivamente la dir. 95/46 alla luce dei diritti di cui agli artt. 7 e 8 della Carta, ha affermato il diritto alla deindicizzazione dei dati personali, riconoscendo che il motore di ricerca è responsabile del trattamento dei dati (par. 32-41), individuando in Google Spain uno stabilimento del responsabile *Google Inc.* e obbligandolo a sopprimere «dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita» (par. 88).

Rappresenta il leading case italiano (Caso Google vs Vividown) sulla responsabilità del provider per illecito trattamento di dati invece, la vicenda giudiziaria originata dalla pubblicazione di un filmato su Google Video che ritraeva un ragazzo disabile bullizzato dai compagni di classe i quali, contestualmente, pronunciavano espressioni ingiuriose nei confronti dell'associazione Vividown. Il tribunale di Milano, all'esito del dibattimento,

[77] Per un approfondimento sulla costruzione del diritto fondamentale alla protezione dei dati personali, si veda L. CALIFANO, -C. COLAPIETRO (a cura di*), Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali. Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, 3 ss

[78] Cort.giust, UE 8-4-2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland, Seitlinger e a.

[79] Cort. giust., UE, 13-5-2014, causa C-131/12, Google Spain, cit.

assolveva i manager di Google tratti in giudizio: nessun obbligo preventivo di impedire gli illeciti degli utenti, fermi i doveri di segnalazione all'autorità[80].

Infine, il 6-10-2015, con la sentenza Schrems[81] la Corte ha invalidato la decisione della Commissione 2000/520, con la quale si riconosceva l'adeguatezza del sistema di protezione dei dati statunitense (c.d. Safe Harbour).

In una sentenza ancora più recente la Corte ha chiaramente affermato che l'art. 8 della Carta riguarda un diritto fondamentale distinto rispetto a quello sancito all'art. 7 della Carta, che non trova alcun equivalente nella Cedu, con ciò consentendo al diritto dell'Unione di concedere una protezione più estesa del diritto di quella offerta dalla Cedu[82].

L'insieme di queste decisioni più recenti[83] sviluppa un secondo e inedito passaggio. Le pronunce in parola, partendo dalla dimensione dinamica del diritto fondamentale europeo alla vita privata, acquisiscono un rilievo ordinamentale. Questa giurisprudenza della Corte coglie la tutela del diritto fondamentale nella sua implicazione rispetto alla architettura della rete internet: dalle decisioni (compresa la recente Tele2 Sverige) sulla data retention discende l'esigenza di disciplinare puntualmente e con maggiori garanzie la conservazione e l'accesso ai dati personali, sia a livello europeo, sia a livello di Stati membri; dalla sentenza Schrems deriva la necessità di regolare nuovamente i rapporti con altri ordinamenti per consentire il trasferimento dei dati personali; dalla stessa decisione Google Spain si inizia a delineare il ruolo e la responsabilità dei motori di ricerca nel contesto della circolazione delle informazioni in rete.

La Corte pertanto sembra tenere ben presente la connessione fra i tre livelli implicati nella regolazione della protezione dei dati personali nella società dei dati che si sono descritti nella parte prima di questo lavoro: il livello di tutela della persona, il livello della tutela degli ordinamenti, il livello della regolazione della architettura della rete internet e cioè della società dei dati. Si tratta di tre aspetti che si implicano a vicenda, nel senso che appare inefficace una tutela del diritto della persona che non implichi anche gli altri aspetti ed è forse questo l'aspetto che più si evidenzia dalle citate sentenze della Corte.

---

[80] Cass. pen., Sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107.

[81] Cort.giust. UE, 6-10-2015, C-362/14, Schrems, cit.

[82] Cort.giust., UE, 21-12-2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB.

[83] S.SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di Sica-D'Antonio-Riccio, Cedam, Milano, 2016, p.4.

Non è un caso che proprio mentre questa giurisprudenza veniva elaborata l'Unione europea stesse discutendo ed approvando il nuovo «pacchetto privacy» europeo.

L'influenza esercitata dallo sviluppo giurisprudenziale delineato è rilevante ed ha accompagnato il percorso seguito dall'ordinamento europeo verso l'armonizzazione e l'unificazione del diritto alla protezione dei dati personali.

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (*GUUE*) i testi del regolamento generale sulla protezione dei dati (che abroga in sostanza la dir. 95/46/CE) e della direttiva che regola i trattamenti di dati personali nella prevenzione, contrasto e repressione dei crimini. Il 5 maggio 2016 è entrata ufficialmente in vigore la Direttiva, che gli Stati membri recepiscono entro due anni.

La lettura dei considerando del regolamento lascia intravedere, con una certa chiarezza, gli obiettivi e le finalità principali che sono alla base del faticoso processo di elaborazione, durato circa un lustro[84].

Appare evidente che il fine del regolamento è garantire il diritto fondamentale sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e ribadito dall'art. 16 TFUE, concernente la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale.

In questa prospettiva, l'esigenza primaria che ha suggerito l'adozione di un nuovo set di regole europee è strettamente legata alla digitalizzazione della società e dell'economia europea (e globale). L'ambiente digitale è costituito dalla produzione, condivisione, elaborazione di un flusso incessante di dati: «*la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività*» e, contemporaneamente, «sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano» (cons. 6).

La circolazione di questa massa crescente di dati è un valore da custodire e promuovere, sia all'interno dell'Unione europea, sia nei rapporti con i «paesi terzi» e con le organizzazioni internazionali, ed appare tuttavia necessitare di nuove ed apposite regole europee volte alla garanzia di un elevato livello di protezione dei dati personali.

[84] S. GUTWIRTH, R.LEENES, P. DE HERT (edited by), Reforming european data protection law, law, governance and technology series, XX, SPRINGER, 2015.

In base all'esigenza di garantire il diritto individuale alla protezione dei dati personali in ambiente digitale, le nuove regole europee perseguono altresì il fine di instaurare quel «clima di fiducia» e di certezza giuridica - fondato sulla consapevolezza delle persone fisiche di avere il controllo sui propri dati personali - necessario per lo «sviluppo dell'economia digitale in tutto il mercato interno» (cons. 7).

Società digitale, certezza giuridica, mercato unico: il perseguimento di questi obiettivi prioritari si lega strettamente con l'altra grande finalità (in qualche modo, strumentale ed operativa) del regolamento europeo: il superamento della frammentazione giuridica delle norme e delle prassi applicative in tema di protezione dei dati personali sul suolo dell'Unione europea[85].

Si può osservare infatti che «sebbene i suoi obiettivi e i suoi principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche». La coesistenza di diversi livelli di protezione a livello nazionale rappresenta un ostacolo alla libera circolazione dei dati personali all'interno dell'Unione, un freno all'esercizio delle attività economiche su scala dell'Unione, un ostacolo alla concorrenza e un intralcio alle autorità nazionali nell'adempimento agli obblighi loro derivanti dal diritto dell'Unione. Si afferma con chiarezza che «tale divario creatosi (…) è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE» (cons. 9).

La conseguenza di tale osservazione è duplice e decisamente rilevante. È stato necessario così utilizzare una "nuova" fonte", il regolamento europeo, ritenuto l'unico in grado di garantire «un livello coerente di protezione delle persone fisiche», certezza del diritto e trasparenza agli operatori economici e di «prevenire disparità» a livello nazionale (cons. 13), anche sotto il profilo sanzionatorio.

[85] D. ERDOS, *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in Journal of Law and Society, 2016.

Fra le ragioni che hanno condotto all'adozione delle nuove regole europee in materia di protezione dei dati personali delle persone fisiche va annoverata, pertanto, anche l'avvertita esigenza di sostituire la fonte regolamentare alla direttiva[86].

È bene sottolineare a questo punto dell'elaborato che, dopo la sentenza del 2015 (per comodità definita "Schrems I") arriva una nuova determinazione della Corte di giustizia in materia di trasferimento dei dati personali dall'Unione europea verso gli Stati Uniti d'America. Sostanzialmente questa sentenza risulta in linea di continuità con il precedente del 2015 ed è coerente anche con le più recenti sentenze della Corte in materia di protezione dei dati.

La sentenza[87] fa seguito al nuovo ricorso presentato da Maximilian Schrems, che chiede al Commissario per la protezione dei dati irlandese di sospendere o vietare il trasferimento dei suoi dati personali effettuato da Facebook Ireland verso la casa madre, Facebook Inc., che si trova negli Stati Uniti.

Assume rilevanza questa pronuncia per il parametro del giudizio preso in considerazione e in essa utilizzato. Nel 2015, infatti, il parametro era rappresentato dalla direttiva 95/46, nella seconda sentenza è il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[88]. Un elemento di novità importante che caratterizza la pronuncia della Corte.

[86] Deve comunque sottolinearsi che, da un lato, il Regolamento europeo appare la fonte del diritto più adeguata per far tesoro dell'ormai ampia elaborazione e dei ripetuti interventi della Corte di giustizia dell'Unione europea, citati nella par. II, par. 11. D'altra parte, è opportuno segnalare che il Reg. UE 2016/679, lascia ampi margini di attuazione a livello statale (cfr., ad es., cons. 8, 10, e artt. 8, 9, 23, 80, 85, 87, 88, 90), seppure nell'ambito di stringenti meccanismi di cooperazione e coerenza (capo VII, artt. 60 ss.) volti ad uniformarne l'applicazione a livello europeo.

[87] Cort. giust UE (Grande Sezione), 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Lts, Maximilian Schrems*

[88] R. BIFULCO, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno.* Diritto Pubblico Europeo - Rassegna Online, 14(2).

1.3 La nuova strategia europea di cybersecurity e il GDPR: quali interazioni.

Ciò che viene ricompreso all'interno della c.d. cybersecurity è una questione di non semplice risoluzione. In letteratura è infatti possibile rintracciare diverse definizioni di questo termine.

Partendo dalle definizioni internazionali, secondo l'Unione internazionale delle telecomunicazioni (2010), la cybersecurity rappresenta «*la raccolta di strumenti, policies, concetti e garanzie di sicurezza, linee guida, approcci di gestione dei rischi, azioni, formazione, best practice, assicurazioni e tecnologie che possono essere utilizzate per proteggere l'ambiente e l'organizzazione informatica e le risorse dell'utente*».

Secondo l'Unione Europea (2013), la cybersecurity si riferisce invece a «*le misure di salvaguardia e le azioni che possono essere utilizzate per proteggere il dominio cibernetico, da quelle minacce che sono associate o che possono danneggiare le sue reti interdipendenti e la sua infrastruttura informativa. La sicurezza informatica si impegna a preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni in esse contenute*»[89].

Tra le fonti italiane, secondo il Framework nazionale per la cybersecurity (2015), è possibile definire la cybersecurity come «*quella pratica che consente a un'entità, ad esempio, organizzazione, cittadino, nazionale etc. la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyberspace*».

Nelle ultime due definizioni compaiono alcuni concetti fondamentali, che torneranno di frequente nel corso dell'elaborato, e con i quali occorre iniziare a prendere familiarità.

Le parole chiave da tenere sempre a mente quando si affrontano tematiche legate alla sicurezza cyber sono: la disponibilità; l'integrità e la confidenzialità che devono caratterizzare non solo i dati e le informazioni, ma anche i sistemi e le reti, perché queste possano ritenersi sicure.

Si tratta della cosiddetta triade CIA (confidentiality, integrity and availability). Una definizione delle singole proprietà è rintracciabile nello standard internazionale in materia di

[89] B.J. KOOPS, S. ADAMS ET AL., *The governance of cybersecurity, Tilburg University TILT* - Tilburg Institute for Law, Technology, and Society, 2015.

Information technology and security (ISO/IEC 27000).

Questi concetti costituiscono il punto di partenza e il parametro di riferimento per la sicurezza informatica, anche se nascono nel contesto più ristretto della sicurezza delle informazioni (Information security), di cui si tratterà in seguito.

Seppur siano concetti fondamentali e necessari, possono risultare a volte, (soprattutto quando si parla di cybersecurity), non sufficienti, ed andranno quindi accostati ad altre caratteristiche che devono caratterizzare le componenti informatiche a cui si rivolge la più ampia sicurezza cyber.

Ulteriori proprietà che definiscono la sicurezza delle informazioni, così come dei dati e delle tecnologie dell'informazione e della comunicazione in generale, sono l'autenticità, proprietà per la quale un'entità è ciò che afferma di essere, la responsabilità e la non-repudiation (letteralmente non-disconoscimento), capacità di provare l'occorrenza dell'evento o dell'azione che si è dichiarato essere occorsa, nonché quali entità lo hanno originato; l'affidabilità, proprietà per cui il risultato e il comportamento sono coerenti e corrispondenti a quelli voluti.

Dalle definizioni generali sopra riportate di cybersecurity è necessario ora ritagliarne una maggiormente precisa, che risulti rilevante e applicabile al contesto delle imprese.

Tralasciamo per un attimo l'oggetto a cui si rivolge la cybersecurity, ossia l'individuazione degli elementi dei quali vuole assicurare la sicurezza, punto che sarà articolato meglio in seguito[90].

Per ora, come punto di partenza, possiamo cominciare a delineare quello che è l'intento, lo scopo della cybersecurity, rilevante ai fini della presente indagine: tutelare l'azienda da eventuali eventi dannosi verificatisi o perpetrati attraverso il funzionamento o l'utilizzo di strumenti informatici. Eventi dannosi di diversa natura e provenienza possono essere i seguenti: attacchi informatici (o cyber) esterni, attacchi informatici (o cyber) interni, incidenti informatici.

Una parte integrante della cybersecurity si è visto essere l'Information security, e, a sua volta, la sicurezza delle informazioni non può che passare attraverso la sicurezza dei dati, specifici elementi che costruiscono la stessa informazione.

La sicurezza dei dati si realizza attraverso l'implementazione di misure volte alla

[90] J. KREMLING, A.M. SHARP PARKER, *Cyberspace, Cybersecurity, Cybercrime*, Sage pubblication, 2018.

preservazione e garanzia della configurabilità, integrità e disponibilità dei dati stessi, i quali devono essere protetti in tutte le fasi in cui vengono utilizzati. Oggi la protezione dei dati (non solo di quelli personali) è una parte essenziale dell'organizzazione di un'azienda, tenuto conto, peraltro, del sempre più largo utilizzo che viene fatto dei Big data[91] e della Big data analytics.

Intendiamo con:

- Big data: i Big data sono beni informativi ad alto volume, ad alta velocità e ad alta varietà, che richiedono forme innovative ed economiche di elaborazione delle informazioni, e che permettono di arrivare a una comprensione approfondita del fenomeno cui si riferiscono, nonché a processi decisionali su quello stesso fenomeno.

Big data analytics è un processo decisionale basato sull'evidenza, tramite il quale elevati volumi di dati veloci e diversificati vengono trasformati in conoscenze rilevanti[92].

Per fare un esempio su tutti dell'utilizzo dei Big data in ambito economico basti pensare alla cosiddetta "data mining", raccolta di dati dagli utenti per comprendere meglio le loro preferenze e comportamenti, cercando di prevedere gli acquisti che faranno e direzionare al meglio le attività di marketing.

Nell'era dei Big data la sicurezza deve coprire tutto il cosiddetto ciclo di valore dei dati, il quale comprende le fasi[93] della: datification e collezione dei dati, la fase di digitalizzazione. la creazione dei Big data, data analytics, creazione di una base di conoscenza, processi decisionali basati sui dati elaboratori e analizzati.

Il modo per garantire una sicurezza dei dati è ricorrendo ad una buona compliance in materia; attraverso quindi misure tecnico-organizzative ideate attraverso un procedimento di valutazione e gestione del rischio.

È opportuno evidenziare, tuttavia, che assumono un ruolo particolarmente significativo i dati personali. A completare dunque il quadro delle normative in materia vi è anche quella parte di disposizioni che disciplinano la sicurezza dei dati personali e del trattamento che viene

---

[91] M.L. MONTAGNANI, M.A. CAVALLO, *Cybersecurity and liability in a Big Data World*, in Market and Competition Law Review, 2018.

[92] A. VISCONTI, *La sicurezza informatica e la rete*, in G. Cassano (a cura di), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, Wolters Kluwer, Milano, 2017, p. 532 ss.

[93] M.L. MONTAGNANI, M.A. CAVALLO, *Cybersecurity and liability in a Big Data World*, op.cit.

fatto degli stessi.

Questa materia ha assunto nel tempo maggiore rilevanza, in virtù del valore che oggi connota i dati personali, i quali sono caratterizzati da un'importante portata economica, andando a costituire in alcuni casi la materia prima del business di alcune imprese, e in altri, una vera e propria merce di scambio.

Il quadro normativo in materia da cui è necessario partire è il Regolamento europeo 2016/679/UE (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)[94].

Come "dato personale" si definisce «*qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

Il termine "trattamento" dei dati si riferisce invece a «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*». [95]

I soggetti interessati da questa normativa sono: il titolare del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali e il responsabile del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

All'interno del Regolamento, sicurezza e privacy, formano un binomio inscindibile: senza l'una non è possibile garantire l'altra, e viceversa. Nella normativa Ue troviamo infatti

[94] R. VON SOLMS, J. VAN NIEKERK, "*From information security to cyber security*", in Computers &security, 2013, n. 38, p. 97 ss.

[95] Art. 4 EU RGPD "Definizioni".

diversi riferimenti alla sicurezza che deve caratterizzare i dati personali e il trattamento che si fa degli stessi.

In particolare, all'art. 5, comma 1, lett. f), il Regolamento stabilisce che i dati personali siano «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*».

La responsabilità del trattamento dei dati ricade sul titolare del trattamento, secondo i dettami del principio della cosiddetta accountability[96].

Il GDPR formalizza un principio di "responsabilizzazione" del titolare del trattamento, a cui è affidato il compito di stabilire, in modo indipendente, le modalità, le garanzie e i limiti del trattamento dei dati, adottando misure adeguate ed efficaci[97].

Dalla generalità dei termini utilizzati si evince come vi sia un ampio margine di discrezionalità in capo al titolare del trattamento.

Il principio è ricavabile dall'art. 24, par. 1 del Regolamento Ue.

Per quanto riguarda la sicurezza dei dati, essa coinvolge sia il titolare che il responsabile del trattamento, e trova la propria disciplina alla Sezione 2 del Capo IV (art. 32 ss.)[98].

In base all'art. 32, par. 1: «*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*».

Il concetto di "rischio" ha un ruolo significativo all'interno del GDPR, è il parametro su cui costruire un sistema organizzativo che tuteli e garantisca la sicurezza dei dati personali[99].

La produzione di un dato digitale porta, infatti, con sé l'inevitabile rischio connesso al trattamento che viene fatto dello stesso: il dato, una volta che è inserito nel circuito digitale,

---

[96] R. RAPICAVOLI, Come applicare il GDPR e il codice privacy negli studi e nelle aziende, Maggioli, Rimini, 2018, p.22,23

[97] M. GRANIERI, *Il sistema della tutela dei diritti nella legge 675/1996*, in AA. VV., Diritto alla riservatezza e circolazione dei dati personali, (a cura di Pardolesi), Milano, 2003, p. 437 ss.

[98] P. A. MAZURIER, *Sul concetto di Cyberterrorismo e la Costruzione della Cyber(in)sicurezza*, Center for Cyber Security and International Relations Studies, Firenze, 2017.

[99] F. PENNAROLA, *Innovazione e Tecnologie Informatiche*, Università L. Bocconi Editore, 2006, p.28 ss.

verrà utilizzato, comunicato, diffuso, incrociato con altri dati e sistemi, per finalità alcune volte imprevedibili.

Per questo le misure che deve adottare il titolare del trattamento devono partire sempre da una valutazione sistematica dei rischi attuali e potenziali del trattamento.

1.4 Direttiva NIS e Cybersecurity Act: due baluardi UE per la sicurezza nazionale

La Direttiva UE/2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione, è attuata nel nostro ordinamento attraverso il NIS.

Ai sensi della Direttiva, sicurezza della rete e dei sistemi informativi significa:

« *capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tali reti o sistemi informatici*»[100].

Da questa definizione cominciamo a vedere lo stretto legame che sussiste tra sicurezza dei dati, dei sistemi e delle reti.

La direttiva ha tre obiettivi principali: migliorare le capacità nazionali di cybersicurezza, rafforzare la cooperazione a livello dell'Ue, promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali.

Le novità introdotte dalla Direttiva possono essere divise in due insiemi.

Da una parte, essa prevede una serie di obblighi di sicurezza per alcune categorie di organizzazioni private; dall'altra parte, ha imposto agli Stati membri di costruire un sistema nazionale per la cybersicurezza volto alla collaborazione e cooperazione a livello internazionale.

Per ciò che interessa le organizzazioni private, la Direttiva si rivolge a due categorie ben precise, ponendo in capo agli stessi alcuni obblighi di sicurezza.

Le imprese interessate dalla Direttiva NIS e dal Decreto legislativo d'attuazione sono innanzitutto, gli operatori di servizi essenziali, ossia soggetti pubblici o privati che forniscono un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali nonché dipendente dalla rete e dai sistemi informativi. Si tratta di quei soggetti che operano nei settori: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distruzione di acqua potabile, infrastrutture

[100] R. BRIGHI, "*La vulnerabilità nel cyberspazio*", in Ars interpretandi, 2017, n. 1, p. 81 ss.

digitali[101]. È compito di ogni Stato identificare, per ciascun settore e sotto-settore, gli operatori di servizi essenziali con una sede nel proprio territorio. L'elenco nazionale degli OSE è istituito presso il Ministero dello sviluppo economico e viene aggiornato, almeno ogni due anni, a cura delle Autorità competenti NIS, (si tratta di lista secretata in quanto contenente informazioni sensibili).

In secondo luogo, i fornitori di servizi digitali: qualsiasi persona giuridica che fornisce un servizio digitale, dove con servizio digitale s'intende qualsiasi servizio della società dell'informazione, ossia qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Un servizio che deve essere ricompreso tra le tipologie di mercato online, motore di ricerca online e servizi della nuvola (cloud computing).

A differenza degli OSE, i FSD non sono censiti singolarmente dalle autorità pubbliche, ma vengono solo individuati per categoria d'appartenenza.

A seguito dell'attuazione operata dal D.Lgs. n. 65/2018, assume un ruolo fondamentale il CSIRT nazionale (computer security incident response team), che diventerà il cardine delle attività di analisi e contrasto e a cui le imprese private devono fare riferimento in caso di attacco o incidente cyber. Il CSIRT italiano è istituito presso la Presidenza del Consiglio dei ministri mediante unificazione del Computer Emergency Response Team (CERT) Nazionale e del CERT-PA, assumendone i compiti.

La conoscenza delle autorità pubbliche di riferimento è di primaria importanza, dal momento che è proprio attraverso la cooperazione tra privato e pubblico che è possibile costruire meccanismi e procedure di gestione e reazione agli attacchi.

Bisogna tenere a mente, come ha sottolineato la stessa Commissione europea, che l'efficacia dei tradizionali meccanismi di contrasto è messa a dura prova dalle caratteristiche del mondo digitale, che consiste principalmente in infrastrutture di proprietà privata e in molti operatori diversi fra loro.

Di conseguenza, per le autorità pubbliche la cooperazione con il settore privato, con l'industria, (ma anche con la società civile), è fondamentale per combattere efficacemente la cyber criminalità.

[101] R. FLOR, "*Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*", in Diritto di Internet, 2019, n. 3, p. 465 ss.

È quindi molto importante che le imprese siano in grado di condividere con le autorità di contrasto informazioni riguardanti incidenti concreti, nel pieno rispetto delle norme in materia di protezione dei dati; soprattutto perché anche le aziende non identificati come OSE, o che non forniscono servizi digitali, possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei propri servizi.

Un'altra fonte normativa europea che va a fondare la strategia europea per la cybersicurezza è il Regolamento 2019/881/UE[102]. Questo strumento normativo in sostanza, si affianca, essendone in parte complementare, alla prima normativa in materia di sicurezza cibernetica introdotta a livello dell'Unione, ossia la Direttiva NIS.

Il Regolamento, con il fine di creare un sistema europeo di certificazione della sicurezza informatica delle tecnologie della comunicazione e dell'informazione (TIC), nonché dei servizi digitali, istituisce il quadro europeo di certificazione della cybersicurezza.

Il quadro prevede, ai sensi dell'art. 46, par. 2, «*un meccanismo volto a istituire sistemi europei di certificazione della cybersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC siano conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, autenticità, integrità o riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita*».

I sistemi di certificazione dovranno essere volti alla protezione dei dati conservati, trasmessi o trattati da: accidentali o non autorizzati trattamenti, accessi o divulgazioni durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC; accidentali o non autorizzate distruzione, perdita o alterazione, oppure dalla mancata disponibilità durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC[103].

[102] Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») GU Serie Generale L 151/15, 7.6.2019, pp. 15–69

[103] M.T. GIORDANO, G. VACIAGO, "*La sicurezza informatica, un asset aziendale strategico*", Milano, 2018, pp. 273-283.

Ma vediamo cosa è accaduto subito dopo, volendo rispettare un ordine cronologico dei fatti. La crisi dovuta all'epidemia da Covid-19, in questi ultimi due anni, come abbiamo avuto modo di trattare, ha reso l'economia dell'UE più dipendente dalla rete e dai sistemi informatici. In alcuni Stati Membri, gli ospedali del sistema sanitario non sono stati inclusi tra i soggetti sottoposti all'obbligo di misure di sicurezza previste dalla NIS, per cui sono stati maggiormente esposti a minacce cibernetiche nel contesto della crisi legata al COVID-19. In sostanza, la pandemia ha confermato la necessità di preparare l'UE per il decennio digitale, nonché di migliorare la resilienza informatica, specie per coloro che gestiscono servizi essenziali come l'assistenza sanitaria e l'energia.

È pur vero che la Direttiva NIS, primo atto legislativo a livello europeo sulla sicurezza informatica, era stata emanata dal Parlamento Europeo per creare un livello comune ed elevato di sicurezza delle reti dei sistemi informativi nella UE.

L'applicazione della Direttiva nei Paesi membri ha incontrato non poche difficoltà che hanno portato la Commissione Europea a richiederne l'abrogazione e l'introduzione della nuova Direttiva "NIS 2" al fine di modernizzare il quadro europeo sulla sicurezza cybernetica. Il nuovo pacchetto di misure per la realizzazione della strategia UE per la sicurezza informatica è stato denominato "EU's Cybersecurity Strategy for the Digital Decade", presentato a dicembre 2020, dalla Commissione Europea e dall'Alto Rappresentante dell'Unione per gli Affari esteri e la politica di sicurezza.

Del resto, le capacità di cybersicurezza degli Stati membri sono aumentate e l'attuazione del provvedimento si è rivelata particolarmente difficile e la conseguenza è stata una frammentazione a vari livelli nel mercato interno.

Da allora, l'Unione europea ha adottato una nuova strategia di sicurezza informatica 2020-2025, che ha proposto la revisione della Direttiva, in linea con le priorità indicate dalla Commissione.

Occorre oggi far fronte ai rischi attuali e alle sfide del futuro. Fondamentale sarà garantire, ad esempio, che la tecnologia 5G risulti sicura ed affidabile.

La nuova proposta include un elenco di sette elementi chiave che tutte le aziende dovranno sostenere o attuare tra le misure che adottano, ivi compresa la risposta agli incidenti, la sicurezza della catena di approvvigionamento, la divulgazione delle vulnerabilità ma anche la crittografia.

Vi sono contenute anche alcune puntualizzazioni sulla segnalazione degli incidenti oltre a stabilire regole e procedure in caso di episodi o crisi su larga scala.

Le aziende interessate hanno 24 ore dal momento in cui vengono a conoscenza di un incidente per presentare per la prima volta un rapporto iniziale, seguito da un rapporto finale entro e non oltre un mese dopo.

Viene stabilita anche una lista minima di sanzioni amministrative ogni volta che gli operatori violano le norme in materia di gestione dei rischi per la sicurezza informatica o i loro obblighi di segnalazione stabiliti nella direttiva NIS.

Il governo italiano, lo scorso giugno, ha definito un allargamento del perimetro della sicurezza informatica nazionale, inserendo nuovi soggetti tra quelli che erogano funzioni essenziali per lo Stato e richiedendo a questi nuovi obblighi in tema di sicurezza.

1.5 Mandato e nuove sfide dell'ENISA (Agenzia dell'Unione Europea per la cybersicurezza)

Il compito di elaborare una proposta di sistema o di rivedere il sistema europeo di certificazione della cybersicurezza esistente spetta all'ENISA, Agenzia che diventerà un punto di riferimento operativo in materia.

Il Regolamento UE 2019/881 conferisce un mandato permanente all'ENISA, che diventa il perno di un sistema europeo di raccolta di informazioni e segnalazioni da parte degli Stati membri: operando in modo indipendente, è chiamata a fungere "da punto di riferimento per pareri e competenze in materia di cybersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione"[104]; inoltre, "sostiene la cooperazione operativa tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e tra i portatori di interessi"[105]. L'Agenzia, così potenziata (anche se, probabilmente, in modo ancora insufficiente, stante la sproporzione dei mezzi rispetto ai fenomeni da fronteggiare), offre un supporto concreto in ordine ai singoli episodi che dovessero interessare uno Stato membro[106].

L'Agenzia ricopre un ruolo chiave, ha il compito di creare le condizioni per consentire un livello comune di cybersicurezza che sia elevato in tutta Europa, incrementando la resilienza delle infrastrutture e garantendo la sicurezza digitale della società e dei cittadini.

Contribuisce alla politica dell'UE in materia di sicurezza nel settore informatico, migliora l'affidabilità dei servizi e dei processi TIC con programmi di certificazione, collabora con gli Stati membri e gli organismi dell'UE ma soprattutto assiste l'Europa nell'affrontare le sfide informatiche del prossimo futuro. Ha già creato la mappa

[104] Art. 1, par. 1, *Reg*. n. 2019/881. L'indipendenza è espressamente richiamata nel testo normativo, al par. 3 dello stesso articolo.

[105] Art. 7, par. 1, *Reg*. n. 2019/881.

[106] Sull'Agenzia, istituita nel 2004 con compiti ben più limitati, si veda D. MARKOPOULOU, V. PAPAKONSTANTINOU, P. HERT, *The Nis Directive, Enisa's role and the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019, p.1 ss. Si rinvia anche a B. Carotti *La collaborazione tra autorità europee delle telecomunicazioni*, Esperia, London, 2011, pp..55 ss.

istituzionale della cybersicurezza in Europa con lo scopo di individuare e far conoscere i principali portatori di interessi.

Vediamo che cosa prevede invece, la nuova normativa italiana in tema di Cyber Security.

Sulla Gazzetta Ufficiale è stata pubblicata la legge 4 agosto 2021, n.109 su "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" che converte il d.l. n. 82/2021.

La legge definisce l'architettura nazionale di cybersicurezza e introduce interessanti novità. Innanzitutto, istituisce l'Agenzia nazionale per la Cybersecurity, il Comitato interministeriale per la cybersicurezza (CIC), il Nucleo per la cybersicurezza.

È nata così in Italia l'Agenzia per la cybersicurezza nazionale (ACN) che opera sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la sicurezza della Repubblica e in raccordo con il Sistema di informazione per la sicurezza della Repubblica. La nuova legge, entrata in vigore il 5 agosto 2021, completa la strategia di cyber-resilienza nazionale, intrapresa con la disciplina sul perimetro cibernetico, e accresce di fatto la consapevolezza del settore pubblico, privato e della società civile su rischi e minacce.

Inoltre, assume una funzione di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi (direttiva NIS) nonchè della sicurezza delle reti di comunicazione elettronica. Alla guida dell'Agenzia (ACN) è stato indicato Roberto Baldoni, già vicedirettore del Dipartimento delle informazioni per la sicurezza (DIS)[107].

Approvato lo scorso settembre anche il decreto del Presidente del Consiglio dei ministri che prevede che il DIS (Dipartimento delle informazioni per la sicurezza) debba assicurare la prosecuzione, non oltre il 31 marzo 2022, dell'erogazione dei servizi informatici necessari alla prima operatività dell'Agenzia, tra cui quelli per garantire la continuità del servizio del Csirt Italia e del perimetro di sicurezza nazionale cibernetica, assicurandone la fruibilità dalla sede dell'Agenzia". L'Agenzia infatti, come da decreto istitutivo prende in carico tutte le funzioni cyber prima in capo al DIS. Nel mese

[107] LA STAMPA, *Caccia agli hacker. "I dati sono salvi" Nominato Baldoni*, di Edoardo Izzo, 6 agosto 2021, p.6

di ottobre 2021, invece il Premier Mario Draghi, con decreto, ha conferito la delega alla cybersecurity al sottosegretario di Stato Franco Gabrielli.

Del resto, negli ultimi anni, l'Europa si è trovata a fronteggiare un'altra crisi dopo quella economica e finanziaria, dovuta al numero sempre crescente di richiedenti asilo e di migranti economici che, soprattutto dal 2014, si riversano attraverso il Mediterraneo sulle coste della Grecia, della Spagna e dell'Italia per poi raggiungere altri stati membri. Contestualmente negli ultimi anni si sono viste crescere posizioni politiche improntate all'euroscetticismo, a volte addirittura favorevoli all'uscita dall'Unione. A tal punto che il Regno Unito ha votato in maggioranza per la c.d. Brexit nel referendum del 23 giugno 2016 e l'Unione si è trovata per la prima volta nella sua storia ultra sessantennale con il recesso di uno Stato membro.[108]

Vedremo anche più avanti come la pandemia da COVID-19 ha fatto emergere la necessità, non più procrastinabile, di una maggiore sicurezza nel mondo digitale. In questo periodo i criminali informatici hanno approfittato, prendendo a bersaglio soprattutto le imprese di commercio e il pagamento elettronico, nonché il sistema sanitario, una minaccia significativa per la sicurezza interna dell'Unione europea e per quella dei cittadini presenti nella rete.

Del resto, gli attacchi informatici non conoscono confini: possono colpire tutti gli strati della società e l'Unione deve essere pronta a reagire nell'eventualità che vengano sferrati colpi più gravi ed impattanti, generando crisi informatiche generalizzate, a livello transfrontaliero e su vasta scala.

Il loro numero e la loro sofisticatezza aumentano velocemente, insieme allo sviluppo di infrastrutture e tecnologie dell'informazione e della comunicazione. Il fabbisogno di conoscenze e competenze in materia di sicurezza informatica rappresentano l'energia che alimenta il motore della cybersicurezza. Da qui la necessità di investire in competenze e talenti ai vari livelli con professionisti altamente qualificati nel settore nell'ambito del sistema europeo.

[108] A.Adam, A.Tizzano, *Lineamenti di diritto dell'Unione europea*, Giappichelli Editore, Torino, pp. 24-25

CAPITOLO SECONDO

IL CYBERCRIME DIVENTA EMERGENZA GLOBALE

SOMMARIO: 2.1 Competenze dell'Unione europea in materia penale - 2.2 I limiti del principio di territorialità nel cyberspace: il locus commissi delicti - 2.3 Attacchi hacker e reati informatici: tra codice penale e regolamentazione UE - 2.3.1 *Phishing e Pharming* - *2.3.2 Malware e Ransomware* - *2.3.3 Dos e DDos e altre tipologie* - 2.4 Il contrasto al cyberterrorismo: la direttiva 2017/541 contro le organizzazioni criminali strutturate.

2.1 Competenze dell'Unione europea in materia penale

La graduale eliminazione dei controlli alle frontiere all'interno dell'Unione europea ha favorito la libera circolazione dei cittadini dell'UE ma, nello stesso tempo, ha reso più facile l'attuazione di attività criminose su scala transnazionale.

Il punto di partenza, tuttavia, è il principio del riconoscimento reciproco ossia la «fiducia fra gli Stati», allorché «*questa nozione, sebbene recente nella costruzione di una giustizia penale europea, rientra nel principio del reciproco riconoscimento, introdotto al punto 33 delle conclusioni del Consiglio europeo di Tampere del 16 ottobre 1999*»[109] .

Nel tempo si è fatto ricorso a misure specifiche per contrastare la criminalità transfrontaliera e il terrorismo a tutela dei diritti delle vittime, degli indagati e dei detenuti nella UE. La base giuridica si fonda proprio sugli articoli da 82 a 86 del trattato sul funzionamento dell'Unione europea (TFUE).

Quando si parla di diritto penale dell'Unione Europea si parte dall'assunto che «in via di principio, la legislazione penale e le norme di procedura penale restano di competenza degli Stati membri»[110].

[109] Avvocato generale Ruiz-Jarabo Colomer, punto 39 delle conclusioni rese l'8 aprile 2008 in causa C-297/07, Bourquain, in Raccolta, p. I9425 ss.

[110] Cort. Giust. CE, sent. 11 novembre 1981, Casati, C-203/80, Racc, p. 2595 ss, punto 27

Da una prima osservazione non sembrerebbe sussistere, infatti, una potestà sanzionatoria penale diretta dell'UE[111] che, non disponendo di proprie norme penali, né di un apparato giudiziario e coercitivo necessario per il cd. "enforcement" dei precetti penali, non può vedersi riconosciuta una competenza autonoma in materia penale ossia, un insieme di norme applicabili senza la mediazione del legislatore interno.

Del resto, non si dispone di un Codice penale europeo né si può parlare di veri e propri reati europei. Esiste però, una "competenza indiretta" in materia penale.

Parlando di rapporti tra diritto dell'Unione Europea e diritto penale, è necessario però tener conto delle innovazioni introdotte dal Trattato di Lisbona approvato nel ottobre 2007 ed entrato in vigore il 1°dicembre 2009.

Il Trattato ha abolito la distinzione in pilastri, pur conservando il dualismo fra il trattato dell'Unione (Tue) e il vecchio trattato sulla Comunità Europea (TCE) denominato Trattato sul funzionamento dell'Unione (TFUE). È proprio l'art. 83 TFUE, a segnare le coordinate dell'intervento dell'Unione Europea in materia penale.

Tuttavia, anche dopo le modifiche introdotte dal Trattato di Lisbona, la competenza dell'Unione Europea in materia penale rimane una competenza indiretta, ossia una competenza a richiedere agli Stati membri l'adozione di norme incriminatrici laddove siano necessarie a tutelare gli interessi dell'Unione stessa. Diversa è la questione se ci riferiamo all'art. 86 TFUE che prevede l'istituzione di una procura Europea, a partire da Eurojust «competente per individuare, perseguire e rinviare a giudizio (...) gli autori dei reati che ledono gli interessi finanziari dell'Unione, quali definiti nel regolamento previsto nel paragrafo 1»[112].

Dagli atti dell'Unione derivano non solo obblighi di criminalizzazione di determinate condotte ma addirittura vincoli spesso dettagliati sulla concreta conformazione dei precetti e addirittura, sulla natura e misura delle sanzioni penali che lo stato è tenuto ad adottare. Questo non comporta alcun effetto diretto per il cittadino che potrà essere assoggettato ad

[111] C. SOTIS, *Il trattato di Lisbona e le competenze penali dell'unione europea*, in *Cass. pen*., n. 3-2010, p. 1146 ss.

[112] F. POCAR, M. TAMBURINI, *Norme fondamentali dell'Unione europea***,** Giuffrè Editore, 2010, p.58.

una sanzione penale lì dove una legge nazionale preveda come reato il fatto da lui commesso. Non si può però non rilevare come gli stati membri tendano in larghissima misura a conformarsi, in maniera spontanea, agli obblighi derivanti dal diritto dell'UE e, in particolare ad adempiere agli obblighi di penalizzazione, anche per evitare le specifiche sanzioni previste dall'ordinamento comunitario in caso di inadempimento. Il legislatore italiano sembra avere largamente recepito le indicazioni contenute in direttive o in decisioni quadro, sia con decreti legislativi sia con apposite leggi formali di attuazione degli obblighi derivanti dal diritto dell'Unione[113].

La competenza dell'Unione si traduce, ex art. 83, par. 1, nell'assumere «norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale» (cd. "competenza penale indiretta autonoma")[114]. In questa nuova prospettiva, «la competenza al ravvicinamento delle legislazioni penali nazionali viene affiancata e non più subordinata alle esigenze di cooperazione».

Tuttavia, la previsione di «norme minime relative alla definizione dei reati e delle sanzioni», deve conformarsi al principio della sussidiarietà. Tale competenza può esternarsi solo negli ambiti individuati dal Trattato quali ad esempio terrorismo, sfruttamento sessuale di donne e minori, traffico di stupefacenti, traffico di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica nonché criminalità organizzata.

Il Consiglio potrebbe poi adottare, a seguito di approvazione del Parlamento europeo, una decisione per individuare altre sfere di criminalità su cui legiferare e non espressamente incluse nell'art. 83 TFUE.

In sostanza, l'Unione europea non avendo il potere di porre in essere fattispecie incriminatrici applicabili agli Stati membri e di stabilire, in via consequenziale, le relative

[113] G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale*, *Milano*, Giuffrè, 2015, p.51-54.

[114] Sul punto L. PICOTTI, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. GRASSO, L. PICOTTI, R. SICURELLA, (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano 2011.p. 207 ss.

sanzioni, è però dotata di una potestà punitiva amministrativa dal momento che può prevedere e applicare sanzioni patrimoniali e interdittive[115].

Partendo da alcune considerazioni di carattere storico possiamo rilevare come il diritto penale sia stato sempre considerato massima espressione della sovranità dello Stato.

C'è da aggiungere che, nel nostro ordinamento, nello specifico, esiste un principio cardine che è l'art. 25 della Costituzione, cd. "riserva assoluta di legge" che non lascia alcuna possibilità ad una potestà normativa penale proveniente da un organismo esterno all'ordinamento.

Negli anni è andata sviluppandosi la necessità per l'Unione di fornire una risposta alle richieste di tutela di valori comunitari. Nei primi anni di vita della Comunità Europea addirittura, si negava qualsiasi competenza della stessa in materia penale, riservata invece a ciascun ordinamento nazionale. Questo nonostante venisse riconosciuto che il diritto comunitario esercitasse un'influenza riflessa sui vari ordinamenti penali nazionali.

Da un lato, infatti, si notò come l'attività delle istituzioni europee facesse emergere nuovi cd. beni giuridici bisognosi di tutela penale[116], dall'altro venne segnalata una sorta di influenza "riflessa" sui sistemi penali nazionali, che si sostanzia negli effetti che una normativa comunitaria extra penale può esercitare sulle norme penali nazionali. Un classico esempio consiste nella possibilità degli atti normativi europei di limitare la sfera applicativa di disposizioni incriminatrici nazionali[117].

Le prime risposte arrivarono dalla giurisprudenza della Corte di Giustizia e progressivamente si superò il concetto che il diritto penale fosse impermeabile a qualsiasi influenza europea.

---

[115] A. BERNARDI**,** *L'armonizzazione delle sanzioni in Europa: linee ricostruttive,* in 'Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale', G. Grasso - R. Sicurella. (a cura di), Milano, 2008, cit., p.444 ss.

[116] I beni giuridici in questione «*possono essere suddivisi in due gruppi. Il primo riguarda una serie di interessi "istituzionali" collegati all'esistenza e all'esercizio dei poteri sovrannazionali. Il secondo gruppo si ricollega invece, a beni giuridici comunitari che emergono dall'attività della Comunità nel suo concreto dispiegarsi*» in G. GRASSO., R. SICURELLA (a cura di), Introduzione - *Lezioni di diritto penale europeo,* Milano, 2007, p.2.

[117] G. GRASSO, *Diritto penale dell'economia, normativa comunitaria e coordinamento delle disposizioni sanzionatorie nazionali,* in Riv. dir. int. privato e processuale, 1987, p. 227-228.

Veniva affidata agli Stati membri l'attuazione di misure repressive per rendere cogenti le norme comunitarie, il che portava con sé come diretta conseguenza l'esigenza di una forte armonizzazione delle legislazioni nazionali.

Come previsto dall'art. 10 TCE[118] il compito degli Stati membri era quello di assicurare il rispetto della normativa europea, attraverso un sistema sanzionatorio repressivo, poteva definirsi come un vero e proprio obbligo in capo ai medesimi in virtù del principio di leale cooperazione.

Proprio a partire da questo principio, peraltro, la stessa giurisprudenza della Corte di Giustizia ha elaborato i requisiti della risposta sanzionatoria fornita dagli Stati membri, la quale deve essere "adeguata"[119].

C'è da aggiungere poi che dichiarando l'assimilazione di un interesse comunitario ad un bene giuridico nazionale, in realtà il legislatore comunitario non fa altro che creare nuove fattispecie incriminatrici[120].

Si noti che «consentendo la repressione di condotte che non avrebbero potuto essere sottoposte altrimenti a sanzione penale, la norma comunitaria assimilatrice viene pertanto ad assumere una seppur mediata funzione incriminatrice»[121], sebbene ciò sia limitato al caso in cui il bene giuridico nazionale assimilato sia punito penalmente all'interno dell'ordinamento nazionale.

Con l'entrata in vigore del Trattato di Lisbona, L'Unione europea ha offerto uno Spazio europeo di libertà, sicurezza e giustizia[122] in cui è assicurata, *inter alia*, "*la*

[118] Attualmente confluito nel nuovo art. 4 c.3 TUE (Trattato sull'Unione Europea): «*In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati*».

[119] Cort. Giust. CE 10.04.1984, von Colson e Kamann, C-14/83).

[120] 120 F. BRICOLA, *Alcune osservazioni in materia di tutela penale degli interessi delle comunità europee*, in AA. VV. Prospettive per un diritto penale europeo, 1968, p.189.

[121] G. GRASSO, *Verso un diritto penale comunitario: i progetti di Trattato concernenti l'adozione di una regolamentazione comune in materia di repressione delle informazioni alle normative comunitarie ed in materia di responsabilità e di tutela penale dei funzionari e degli altri agenti della Comunità,* in Riv. it. dir. proc. pen., 1982, p.629-637.

[122] U. DRAETTA, N. PARISI, D. RINOLDI (a cura di), *Lo spazio di libertà, sicurezza e giustizia dell'Unione Europea. Principi fondamentali e tutela dei diritti*, 2008, Editoriale Scientifica.

prevenzione della criminalità e la lotta contro quest'ultima" (art. 3, par. 2, TUE) pertanto, "si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità" (art. 67, par. 3, TFUE) ed un'efficace azione di contrasto sia attraverso il coordinamento e la cooperazione tra forze di polizia e autorità giudiziarie, sia tramite il riconoscimento reciproco delle decisioni giudiziarie e, se necessario, il ravvicinamento delle legislazioni penali (art. 67 TFUE).

In questo quadro normativo è da ritenere che, l'intervento de quo dell'Unione europea si sia tradotto, in un primo momento, nell'emanazione di azioni comuni e decisioni quadro, dovute all'esigenza di armonizzazione sistemi nazionali diversi e contrastare la criminalità, in un'ottica di cooperazione e mutuo riconoscimento delle decisioni giudiziarie. Si è poi perfezionato nel tempo grazie ad ulteriori strumenti di cooperazione, tramite regolamenti e direttive.

In sostanza, si può affermare che l'art. 3, par. 2, del trattato sull'Unione europea (TUE) mira a definire gli obiettivi principali perseguiti dall'UE, attribuisce priorità ad uno spazio di libertà, sicurezza e giustizia (SLSG) rispetto al precedente trattato di Nizza.

Il titolo V del trattato sul funzionamento dell'Unione europea (TFUE), artt. da 67 a 89, è dedicato proprio all'SLSG[123] In aggiunta alle disposizioni generali, questo titolo contiene capitoli specifici in materia di politiche relative ai controlli delle frontiere, all'asilo e all'immigrazione, cooperazione giudiziaria in materia civile, cooperazione giudiziaria in materia penale, cooperazione di polizia.

Il TFUE ha inoltre introdotto una serie di clausole da applicare nel caso in cui uno Stato membro ritenga che un progetto di atto legislativo incida su aspetti fondamentali del proprio ordinamento giuridico penale (art. 82, par. 3, TFUE), nonché norme minime comuni relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentino una dimensione transnazionale (art. 3, par. 3, TFUE).

[123] Il TFUE ha inoltre introdotto una serie di «clausole con freno di emergenza» applicabili qualora uno Stato membro ritenga che un progetto di atto legislativo incida su aspetti fondamentali del proprio ordinamento giuridico penale.

In base all'art. 67 TFUE l'Unione realizza uno spazio di libertà, sicurezza e giustizia nel rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri. Si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali. L'Unione facilita l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia civile.

Tra l'altro, nel maggio 2021, l'UE ha adottato le sue priorità in materia di lotta alla criminalità organizzata per i quattro anni successivi, nell'ambito della "piattaforma multidisciplinare europea di lotta alle minacce della criminalità" (EMPACT).

È controverso se l'obbligo per il giudice di disapplicare la disciplina nazionale incompatibile con una norma UE dotata di efficacia diretta sussista anche qualora esso si ponga in contrasto con un principio cardine dell'ordinamento interno: ossia se lo stato membro possa paralizzare quell'obbligo opponendovi l'esigenza di rispettare la propria "identità costituzionale" o meglio, se lo Stato membro possa azionare come "contro-limiti" i principi appartenenti alla struttura fondamentale dello Stato stesso. In questo ambito il caso-guida è rappresentato dal "caso Taricco".

La Corte costituzionale è stata chiamata a decidere se azionare il principio di legalità ex art.25 co.2 Cost, come contro-limite rispetto all'obbligo di disapplicare la disciplina della prescrizione del reato contenuta negli artt.160 co.3 e 161 co.2 c.p., nella misura in cui, quella disciplina è stata ritenuta dalla Corte di Giustizia UE in contrasto con l'art. 325, par. 1 e 2 TFUE (Corte Cost., ord 26 gennaio 2017, n.24)[124].

[124] La Corte Costituzionale, con l'ordinanza in questione, condividendo nella sostanza talune obiezioni dei giudici a quibus, ha optato per una soluzione dialogica, rinviando in via pregiudiziale la questione alla Corte di Giustizia avanzandole in pratica la richiesta di avallare una lettura "costituzionalmente conforme" della sentenza Taricco, che consentisse di superare i dubbi sollevati dai giudici italiani rimettenti.

In un primo tempo la Corte si è espressa con una pronuncia interlocutoria investendo, in via pregiudiziale, della questione la Corte di Giustizia UE, ai sensi dell'art. 267 TFUE.

La Corte costituzionale ha avanzato una specifica richiesta alla Corte di giustizia circa l'interpretazione da dare all'art. 325, par. 1 e 2 TFUE (Corte cost., ord. n.24/2017).

La Corte di giustizia ha risposto[125] che il giudice nazionale non è tenuto a disapplicare le «disposizioni interne sulla prescrizione, rientranti nel diritto sostanziale nazionale, che ostino all'inflizione di sanzioni penali effettive e dissuasive in un numero considerevole di casi di frode grave che ledono gli interessi finanziari dell'Unione europea o che prevedano, per i casi di frode grave che ledono tali interessi, termini di prescrizione più brevi di quelli previsti per i casi che ledono gli interessi finanziari dello Stato membro interessato, a meno che una disapplicazione siffatta comporti una violazione del principio di legalità dei reati e delle pene a causa dell'insufficiente determinatezza della legge applicabile, o dell'applicazione retroattiva di una normativa che impone un regime di punibilità più severo di quello vigente al momento della commissione del reato».

In questo modo la Corte di Giustizia ha riconosciuto che il diritto della UE incontra un limite nei principi di legalità e irretroattività in materia penale che appartengono alle tradizioni costituzionali comuni agli Stati membri.

In sostanza, il giudice nazionale deve verificare, caso per caso, la compatibilità tra gli obblighi che derivano dal diritto dell'Unione e i principi costituzionali. Un secondo vincolo è relativo all'obbligo di interpretazione conforme alla normativa europea. Il giudice nazionale deve interpretare la normativa nazionale che attua gli obblighi di fonte UE, in senso conforme o meglio maggiormente conforme alle pretese del diritto dell'Unione.

Tuttavia, è innegabile che una più esplicita apertura alla materia penale europea si ebbe, prima con il Trattato di Maastricht e successivamente con quello di Amsterdam, i quali assegnavano alla Comunità il compito di emanare provvedimenti atti alla tutela dei propri interessi ed idonei a garantire, tra l'altro, un coordinamento delle attività di polizia e

[125] Cort. Giust. UE, 5 dicembre 2017, M.A.S. e M.B., causa C-42/17 sent. c.d. Taricco bis)

giudiziarie (cd. terzo pilastro). Proprio partendo da questo assunto si delineava un carattere sempre più "ultra-nazionale" della giustizia penale.

Fino ad arrivare alle Agenzie per la cooperazione giudiziaria in materia penale e altri organismi connessi: l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e la Procura europea (EPPO).

Un organismo con la finalità di stimolare e migliorare il coordinamento di indagini e azioni penali tra le autorità giudiziarie competenti degli Stati membri fu proprio Eurojust, istituito nel 2002. L'obiettivo è la lotta alla criminalità organizzata e transfrontaliera.

Con sede a L'Aia (Paesi Bassi), Eurojust oltre a stimolare e migliorare il coordinamento delle indagini e delle azioni penali favorisce la cooperazione tra le autorità degli Stati membri. Agevola l'esecuzione delle richieste di assistenza giudiziaria internazionale e reciproca e l'attuazione delle richieste di estradizione.

È in grado di assistere uno Stato membro che ne faccia richiesta nel quadro di indagini e azioni penali riguardanti lo Stato membro in questione e un paese terzo, se Eurojust ha stipulato con il paese terzo un accordo di cooperazione o se viene dimostrato un interesse essenziale.

Eurojust contempla gli stessi tipi di reati per i quali è competente l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol)[126] come il terrorismo, il traffico di stupefacenti, la tratta di esseri umani, la contraffazione, il riciclaggio di denaro, la criminalità informatica, i reati contro il patrimonio o i beni pubblici, compresi la frode e la corruzione, i reati che ledono gli interessi finanziari dell'UE, i reati ambientali e la partecipazione a un'organizzazione criminale.

Europol fornisce assistenza ai 27 Stati membri dell'Unione europea nella loro lotta contro la grande criminalità internazionale e il terrorismo. L'agenzia collabora anche con molti Stati partner non membri dell'UE e con organizzazioni internazionali.

[126] L'Agenzia Europol istituita con nuovo regolamento sostituisce e assume le funzioni dell'Ufficio Europol istituito con la decisione 2009/371/GAI, pertanto abrogato. La base giuridica è l'articolo 88 del Trattato sul funzionamento dell'Unione europea (TFUE), che prevede che Europol sia disciplinato mediante regolamento da adottarsi secondo la procedura legislativa ordinaria.

Incaricata di svolgere indagini, esercitare l'azione penale e amministrare la giustizia su reati contro il bilancio dell'UE quali la frode, la corruzione o le frodi transfrontaliere in materia di IVA aventi un valore superiore a 10 milioni di EUR è invece l'EPPO[127].

Dal 1° giugno 2021 la Procura Europea (EPPO), con sede in Lussemburgo, è divenuta operativa, incaricata di vigilare sull'utilizzo dei fondi europei e combattere frodi e corruzione dopo la sua istituzione nel 2017 (Reg. 2017/1939 del 12/10/2017) con il compito di curare le indagini e perseguire i reati commessi dalla criminalità finanziaria transfrontaliera.

Oggi tende ad assumere una maggiore rilevanza per la corretta attuazione del Next Generation EU, aprendo le porte ad una nuova fase nella storia dell'integrazione europea.

I componenti della Procura provengono da 22 Stati, con lo scopo di far fronte a quelle frodi internazionali ai danni dell'Unione Europea aventi carattere transfrontaliero e rispetto alle quali le procure nazionali non si ritiene abbiano poteri di indagine sufficientemente rapidi e penetranti.

È stata istituita con una procedura di cooperazione rafforzata (art. 86 TFUE), che consente ad almeno nove Stati membri di instaurare tra loro una cooperazione in un determinato ambito interno alla struttura dell'Unione, senza il necessario coinvolgimento degli Stati che non intendono aderirvi.

In Italia, sono nominati con decreto del 15 aprile 2021 venti procuratori europei delegati, dislocati nei nove uffici territoriali di Bari, Bologna, Catanzaro, Milano, Napoli, Palermo, Roma, Torino e Venezia.

Si tratta della prima procura sovranazionale con funzioni di indagine e potere di azione penale, indipendente dai singoli Stati che non accetta intromissioni esterne, agisce

[127] Il Parlamento e il Consiglio hanno nominato di comune accordo il primo procuratore capo europeo, Laura Codruța Kövesi, per un mandato non rinnovabile di sette anni. Consiglio dell'Unione Europea, comunicato stampa del 14 ottobre 2019; https://www.consilium.europa.eu/it/press/press-releases/2019/10/14/eu-public-prosecutor-s-office-eppo-laura-codruta-kovesi-to-become-the-first-european-chief-prosecutor/

nell'interesse dell'intera Unione e i suoi procuratori sono completamente indipendenti dalle procure nazionali.

La Procura Europea esercita i propri poteri nel perseguire le frodi e altri reati in danno degli interessi finanziari dell'Unione. Sono di competenza della Procura Europea i reati che ledono gli interessi finanziari dell'Unione, come delineati nella direttiva UE 2017/1371 (nota come direttiva "PIF"[128] e recepita con D.lgs.75/2020) che definisce il vasto ambito della nozione di "frode e lesione degli interessi finanziari dell'UE" .

Perché si abbia la competenza territoriale della EPPO (art. 23 Reg. 2017/1939) devono ricorrere i seguenti presupposti: reati commessi in tutto o in parte nel territorio di uno o più Stati membri, reati commessi da un cittadino di uno Stato membro, a condizione che uno Stato membro sia competente per tali reati quando sono commessi al di fuori del suo territorio e infine, deve trattarsi di reati commessi al di fuori degli Stati membri, da una persona che al momento del reato era soggetta allo statuto o al regime applicabile, a condizione che uno Stato membro sia competente per tali reati quando sono commessi al di fuori del suo territorio.

Gli Stati membri che hanno aderito alla cooperazione rafforzata e che hanno designato i propri candidati procuratori, sono attualmente ventidue, (Austria, Belgio, Bulgaria, Cipro, Croazia, Estonia, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Repubblica ceca, Romania, Slovacchia, Spagna, Slovenia) con possibilità in futuro di estendere la cooperazione ad ulteriori adesioni.

Occorre analizzare ora il ruolo del Parlamento europeo fondamentale nella definizione della legislazione dell'UE nel settore della cooperazione giudiziaria in materia penale che ha posto nella sua agenda la lotta alla criminalità e alla corruzione come una

[128] Con il Decreto Legislativo n. 75 del 14 luglio 2020 è stata recepita nell'ordinamento italiano, la Direttiva (UE) 2017/1371 (cosiddetta Direttiva PIF il cui acronimo sta a significare *Protezione Interessi Finanziari*) del Parlamento europeo e del Consiglio del 5 luglio 2017, recante norme per la "*lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*". La Direttiva costituisce un altro passo in avanti verso l'armonizzazione delle misure in materia di tutela degli interessi finanziari dell'Unione Europea, iniziato con la ratifica ed esecuzione della legge n°300/2000, attraverso la quale, nel nostro ordinamento, è stata introdotta la responsabilità penale (rectius amministrativa) anche in capo alle persone giuridiche (D.lgs. 231/2001).

priorità politica su un piano di parità con il Consiglio mentre Eurojust rappresenta lo strumento principale per conseguire la cooperazione giudiziaria in materia penale tra gli Stati membri.

Sicuramente nell'ambito della riforma di Eurojust, il Parlamento ha sostenuto un maggior controllo parlamentare e migliori norme in materia di protezione dei dati.

Risale al 1º dicembre 2020 la prima riunione interparlamentare di commissione sulla valutazione delle attività di Eurojust, in base all'articolo 85 del TFUE e del regolamento (UE) 2018/1727, che il Parlamento ha organizzato sia pure con una partecipazione a distanza a causa della pandemia da COVID-19.

Il 20 gennaio 2021 il Parlamento ha adottato una risoluzione sull'attuazione del mandato d'arresto europeo e delle procedure di consegna tra Stati membri (approvando anche una relazione sull'attuazione della decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, adottata prima del trattato di Lisbona).

Il 28 aprile 2021, invece il Parlamento ha approvato una proposta di regolamento sulla prevenzione della diffusione di contenuti terroristici online, che obbligherebbe le piattaforme Internet a rimuovere i contenuti segnalati o a disabilitarne l'accesso in tutti gli Stati membri entro un'ora dal ricevimento di una richiesta di rimozione.

Il Parlamento seguirà inoltre le recenti e future iniziative della Commissione nei settori del riciclaggio di denaro e del finanziamento del terrorismo, della criminalità organizzata e della criminalità informatica, dei diritti delle vittime, della digitalizzazione della giustizia, della formazione giudiziaria, dell'evoluzione dello Stato di diritto nel settore della giustizia e dell'incitamento all'odio online.

In riferimento alla lotta ai reati e alle minacce pan-UE il Parlamento ha adottato misure specifiche per combattere il terrorismo, la criminalità transnazionale, la corruzione, la frode e il riciclaggio di denaro e per tutelare i diritti delle vittime, degli indiziati e dei detenuti in tutta l'UE.

2.2 I limiti del principio di territorialità nel cyberspace: il locus commissi delicti

L'Unione europea ha fornito una definizione di cyber-security di carattere generale affermando che essa è l'insieme di «safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and informationinfrastructure».

È evidente come il concetto di cyber security e quello di cyber crime siano strettamente collegati. A livello internazionale, la Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 fa riferimento ad un elenco da ritenersi non tassativo di attività riconducibili a crimini informatici come la violazione di contenuti e del diritto d'autore, l'acquisizione di dati riservati, la frode e la pedopornografia. La Convenzione sulla criminalità informatica è l'unico strumento internazionale vincolante in tale ambito e costituisce una guida per ogni Paese che desideri elaborare una legislazione completa per combattere la criminalità informatica, nonché un quadro per la cooperazione tra i suoi Stati parti.

Ritroviamo un'elencazione di reati classificati come cyber crimes anche nel Manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (The United Nations Manual on the Prevention and Control of Computer Related Crime) che include frode, contraffazione e accesso non autorizzato.

Solitamente i cyber crimes vanno distinti dai cyber attack anche se i due termini vengono spesso equiparati. L'attacco informatico rappresenta sempre un'azione attraverso l'uso di computer e networks ma l'obiettivo è di indebolire o neutralizzare i sistemi computerizzati che sono oggetto di attacco e compromettere la sicurezza nazionale di un Paese.

Sono però da escludere da questa categoria tutti quei sistemi considerati di difesa passiva e spesso utilizzati dagli Stati, come i software antivirus o i firewalls. Ma veniamo alla consumazione del reato, argomento che più ci interessa a questo punto della trattazione.

Ogni reato presenta una propria collocazione spazio-temporale da cui derivano determinati effetti inerenti alla successione di leggi nel tempo, alla legge territorialmente applicabile, nonché alla prescrizione del reato.

Una premessa è d'obbligo anche se può risultare scontata: da un punto di vista penalistico Internet ha generato una nuova dimensione e problematiche che devono trovare una propria soluzione sul piano giuridico.

L'autore, soggetto attivo del reato, si avvale di Internet per accrescere la diffusività del proprio messaggio e nascondersi dietro l'anonimato oppure si avvale di quella impunità che a volte può essere offerta dalle leggi del luogo in cui agisce.

Ogni ordinamento giuridico deve introdurre dei limiti di efficacia alla propria esplicazione sia a livello temporale che territoriale, al fine di individuare la fattispecie criminosa in un arco temporale e spaziale. Ecco perché l'esatta individuazione del locus commissi delicti pone dei problemi sia da un punto di vista sostanziale, sia processuale. La questione non riguarda solo l'individuazione del giudice competente, ma concerne la stessa rilevanza penale del fatto ed è diretto a dirimere contrasti giurisdizionali[129].

Se la condotta venisse punita penalmente solo in Italia, ad esempio, la conseguenza sarebbe che, qualora si escludesse l'applicazione della legge italiana, il crimine resterebbe comunque impunito.

Nelle truffe portate a termine con il ricorso al mezzo informatico, la comunicazione a distanza riesce particolarmente efficace quale modo per indurre nella vittima una falsa rappresentazione della realtà[130].

Altri esempi di rilievo si rinvengono nella propaganda di idee a cui i singoli ordinamenti possono attribuire rilievo penale , o nell'abuso dei mezzi di pagamento[131], nel

[129] D. PETRINI, *La responsabilità penale per i reati via internet*, Jovene, 2004, 214 ss.

[130] Cass. pen, Sez. II., Sentenza 6 settembre 2018, n. 40045, in tema di truffa tramite il mezzo informatico. Il soggetto attivo induceva le vittime ad effettuare trasferimenti di denaro su una carta prepagata dopo averli indotti in errore offrendo loro oggetti posti in vendita su Internet e prestando garanzie sulla propria affidabilità di venditore.

[131] R. FLOR, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in Rivista italiana di diritto e procedura penale, 2007, Giuffrè, p. 899 ss.

cyber-terrorismo[132], oppure nel reato di diffusione illecita di immagini o video sessualmente espliciti (art. 612-ter cod. pen.).

In particolare, per poter inquadrare il tema della giurisdizione e della competenza si rendono necessarie alcune considerazioni. Per quanto concerne l'individuazione del luogo di commissione del reato, occorre tenere presente che, generalmente si tratta di accessi virtuali o a distanza attraverso un collegamento effettuato con un modem. Di conseguenza il reato deve ritenersi perfezionato nel luogo in cui ha sede il sistema oggetto di intrusione e non nel luogo in cui si trovi fisicamente l'agente nel momento in cui ha posto in essere le attività contestate[133].

Secondo la giurisprudenza[134] il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico non è quello in cui vengono inseriti i dati idonei ad entrare nel sistema ma quello in cui è ubicato il server che elabora e ispeziona le credenziali di autenticazione del cliente.

Il cyberspace, infatti, viene spesso descritto come un "wild – west". Si tratta di uno spazio che, oltre ad essere in continua ampliamento, consente la delocalizzazione delle risorse, e la detemporalizzazione delle attività.

L'utente può pianificare le operazioni e fare in modo di effettuarle da remoto, senza necessità di alcun contatto fisico tra la persona e il sistema informatico. La deterritorializzazione dell'utente permette di essere presente in più luoghi virtuali.

Internet tende ad ignorare i confini territoriali ma, al contempo, gli ordinamenti necessitano di uno spazio sul quale esercitare la propria sovranità esclusiva. Vediamo cosa accade nell'ordinamento italiano.

Secondo l'art.3 del c.p. (c.d. obbligatorietà della legge penale) «*la legge penale italiana obbliga tutti coloro che, cittadini o stranieri, si trovano nel territorio dello stato* (…) *La legge penale italiana obbliga inoltre tutti coloro che, cittadini o stranieri, si*

[132] R. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in, Diritto penale e modernità. Nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, Napoli, 2017, p. 354

[133] C. PARODI, A. CALICE, *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001, pag. 67.

[134] Cass.pen., Sez. I, 27 maggio 2013, n. 40303.

trovano all'estero, ma limitatamente ai casi stabiliti dalla legge medesima o dal diritto internazionale».

L'art. 6 c.p. (reati commessi nel territorio dello Stato) aggiunge: «*Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana. Il reato si considera commesso nel territorio dello Stato quando l'azione o l'omissione che lo costituisce è ivi avvenuta in tutto o in parte o si è ivi verificato l'evento che è la conseguenza dell'azione o dell'omissione*».

Considerata la dimensione transnazionale degli illeciti, si dovrà anzitutto stabilire a che condizioni un reato informatico possa considerarsi commesso in Italia. La questione risulta quanto mai problematica specialmente in relazione ai reati di pura condotta. «La competenza per territorio è determinata dal luogo in cui il reato è stato consumato». (art.8, comma 1, c.p.p.)».

«*Se la competenza non può essere determinata a norma dell'articolo 8, è competente il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione*».

Se il luogo non è noto «la competenza appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335». (Art.9 c.p.p.).

Per quanto riguarda la competenza per i reati realizzati all'estero «*se il reato è commesso interamente all'estero, la competenza è determinata successivamente dal luogo della residenza, della dimora, del domicilio, dell'arresto oppure della consegna dell'imputato. Nel caso di pluralità di imputati, procede il giudice competente per il maggior numero di essi (…*)» (art. 10 c.p.p.).

Negli altri casi la competenza è attribuita al giudice del luogo in cui l'ufficio del p.m. ha sede e che per primo ha proceduto all'iscrizione della notizia di reato nel registro previsto ex art. 335. Se, invece, il reato è stato commesso solo in parte in territorio estero, la competenza viene determinata a norma degli articoli 8 e 9. Ciò riguarda sicuramente il diritto penale tradizionale, ma diverso può essere il caso che fa riferimento ai nuovi reati cibernetici. Difficile in questo caso delineare a priori la dinamica della tipologia di illecito e complicato risulta individuare i confini temporali, nonché la connotazione spaziale del reato commesso nel cyberspace.

Ebbene, sia per la determinazione della giurisdizione sia per la competenza, è necessario stabilire in modo preciso il locus commissi delicti. La peculiarità della rete sta nel fatto che l'accesso alle informazioni in essa contenute è possibile da ogni terminale/nodo di accesso, sebbene i dati siano "fisicamente" registrati su server collocati in luoghi diversi, a volte anche molto distanti.

Di qui la necessità di stabilire quale sia il momento rilevante per individuare il luogo di commissione del reato (accesso alla rete, accesso al client del server, accesso allo storage server). Innanzitutto è bene sottolineare come il problema si pone per quei reati di evento c.d. informatico e quelli a mera condotta commessi online (ad esempio l'accesso abusivo ad un sistema informatico a distanza, la diffusione di un virus, l'intercettazione di comunicazioni telematiche nonché, la distruzione di dati o programmi informatici sul cloud) ma anche nell'ipotesi di un tentativo di commissione di un reato di evento realizzato online (come il tentativo di truffa o di frode informatica ad esempio).

In breve, la questione si pone per i reati riconducibili alla categoria dei cybercrime, per i quali l'utilizzo della rete Internet e la dispersione di informazioni non consente di stabilire con esattezza quale sia il luogo esatto di consumazione del reato.

Sul punto la giurisprudenza si è dimostrata piuttosto altalenante, fino a trovare una posizione più precisa solo grazie all'intervento delle Sezioni Unite nel 2015 a proposito del luogo di commissione del delitto di accesso abusivo ad un sistema informatico o telematico (Cass.Pen. Sez.Un., 24 aprile 2015, N. 17325)[135].

La Prima Sezione della Corte di Cassazione aveva rimesso alle Sezioni unite il seguente quesito: «*se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter, cod. pen., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente*».

[135] Il contrasto giurisprudenziale aveva avuto origine da un conflitto negativo di competenza sollevato dal GUP presso il Tribunale di Roma in un procedimento che verteva sul reato di accesso abusivo al sistema informatico del Ministero dei Trasporti. (Cass pen. Sez. Un., 24 aprile 2015, n. 17325)

La Suprema Corte, ha risolto così il contrasto: «il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter c.p.[136], è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente». La competenza territoriale nel luogo ove è collocato il server era stata esaminata, prima della pronuncia del 2015, da una sola sentenza della Corte di Cassazione (Cass.pen. 27 maggio 2013, n. 40303)[137].

Ciò che assume rilevanza ai fini dell'integrazione del delitto è il momento in cui l'agente interagisce con il sistema informatico o telematico altrui, si introduce in esso contro la volontà dell'altro. Da ciò ne deriva che l'accesso si individua esattamente nel luogo in cui si supera la barriera di protezione informatica e si entra nel sistema e, quindi, dove è materialmente situato il server oggetto di violazione.

Nel caso in cui si abbia un accesso da remoto, l'attività fisica viene esercitata in un luogo diverso da quello in cui si trova il sistema informatico o telematico oggetto di protezione, ma è certo che il client invia le chiavi logiche al server web che le riceve 'processandole' nella fase di validazione che è eseguita esclusivamente all'interno dell'elaboratore presidiato da misure di sicurezza.

Un sistema telematico deve considerarsi unitario in quanto coordinato da un software di gestione che presiede al funzionamento della rete, alla condivisione della banca dati, alla

[136] Art. 615 ter c.p.: «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».

[137] Cass. Pen., Sez. I, 27 settembre 2013 (ud. 27 maggio 2013), n. 40303 Presidente Chieffi, Relatore La Posta, depositata il 27 settembre.

archiviazione delle informazioni trattate, nonché alla distribuzione e all'invio dei dati singoli terminali interconnessi. Fondamentale per la configurabilità del reato è che il sistema 'vulnerato' risulti protetto da misure di sicurezza[138].

Questo elemento ha creato problemi interpretativi in dottrina e giurisprudenza, visto che il legislatore non ha specificato né la natura né l'intensità delle misure di sicurezza[139].

Le due condotte sanzionate dalla norma ("chiunque abusivamente si introduce…ovvero vi si mantiene") sono formulate in maniera alternativa dal momento che l'intrusione abusiva può realizzarsi solo a seguito di un accesso illecito, viceversa, la permanenza non autorizzata può realizzarsi solo a seguito di un accesso lecito.

Per quanto riguarda il bene giuridico tutelato si ritiene sia il domicilio informatico, ovvero il diritto disporre, godere e controllare le informazioni, i dati e i sistemi in capo al titolare dello "spazio informatico"[140]. Occorre distinguere, però, il reato in questione dalla fattispecie di violazione di domicilio disciplinata dall'art. 614 c.p. Ai fini della configurabilità del reato di accesso abusivo a sistemi informatici o telematici, infatti, si fa riferimento anche a misure di sicurezza "fisiche", ma è necessario che si riferiscano alle modalità di utilizzo di un sistema.

Si pensi, ad esempio, alle misure previste all'interno di un'azienda che richiedano un badge per accedere nell'area dove si trovano i computer, solo in questo caso le misure di sicurezza possono ritenersi espressamente poste per impedire un uso abusivo del sistema.

L'accesso abusivo, dal punto di vista soggettivo, richiede che sussista il dolo generico, o meglio è necessario che il soggetto sia perfettamente consapevole di introdursi o di permanere all'interno di un sistema protetto da misure di sicurezza contro la volontà del titolare dello *ius excludendi alios*. Pertanto, non ha rilevanza il fine a cui è diretto

---

[138] G. AMATO, V.S. DESTITO, G. DEZZANI, C. SANTORIELLO, *I reati informatici*, Cedam Milano, p.47

[139] G. PESTELLI, *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico*, in Cass. Pen., 2012, 6, p. 2330.

[140] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Il diritto penale dell'informatica nell'epoca di Internet, Padova, 2004, 21 e ss.

l'accesso abusivo o la permanenza nel sistema, né il motivo per cui il soggetto ha posto in essere la condotta.

Si è avuto modo di notare che il continuo progredire della Rete è stato considerato un terreno fertile per i cybercriminali.

Insomma, gli interventi legislativi volti ad affrontare il fenomeno hanno portato all'incriminazione di nuove tipologie di condotte, senza considerare le problematiche legate alla particolare modalità con cui avvengono, che rendono ardua l'applicazione dei principi dell'ordinamento tradizionali.

Le condotte si traducono, difatti, in una serie di operazioni automatizzate, che si snodano nei diversi punti della rete e ciò rende problematica la collocazione spaziale del punto in cui il reato si considera consumato.

È bene ricordare la teoria utilizzata dallo stesso legislatore al fine di individuare il locus commissi delicti, cosiddetta teoria dell'ubiquità, per cui il reato si considera commesso nel territorio dello Stato sia se qui è avvenuta parte dell'azione sia se ivi si è verificato l'evento. Se ne deduce che è proprio il particolare modus operandi dell'azione che rende doverosa l'individuazione di peculiari criteri.

A ciò va aggiunto che tale problematica si è posta non per tutte le categorie di illecito che coinvolgono sistemi informatici o telematici, bensì come abbiamo visto, solamente per i reati a evento c.d. informatico, i reati di mera condotta commessi online, nonché per le ipotesi di tentativo di reati di evento commessi online, per cui la condotta o l'evento realizzatosi in Rete e, in particolare, le tecniche di automazione, determinano la circolazione e la permanenza dei dati nello spazio cibernetico, tale da non rendere facilmente identificabile il luogo esatto in cui il reato si è consumato.

Da qui la nascita di voci autorevoli che hanno evidenziato la necessità di un diritto giudiziale flessibile, alla luce del contesto transnazionale, immateriale e aterritoriale in cui i cybercrimes si trovano ad operare.

Ciò ha spinto la giurisprudenza a farsi carico della questione sollevata, con l'intento di fornire soluzioni che potessero risultare confacenti alla luce della struttura atipica che

l'illecito acquisisce nel contesto del cyberspace. Di qui la nascita di orientamenti diversi nel tentativo di dare una risposta adeguata alle caratteristiche della Rete.

Da un lato, assistiamo ad un orientamento legato alla fisicità dei comportamenti ove il luogo di consumazione è legato all'allocazione spaziale del server centrale; dall'altro, un orientamento che privilegia la struttura della Rete, individuando il luogo del commesso reato nel luogo ove l'agente fa partire il dialogo con il sistema informatico.

Davanti a queste due ipotesi la giurisprudenza di legittimità ha privilegiato la struttura unitaria della Rete e il principio del giudice naturale precostituito per legge, preferendo prendere a riferimento il luogo ove è allocato il client anche se tale risposta non sembra soddisfare a pieno viste le peculiarità delle azioni criminose commesse nel cyberspazio che talvolta non permettono di individuare il luogo da cui parte l'azione che coinvolge il sistema.

Peraltro, questa soluzione non è l'unica prospettata visto che il principio espresso dalla giurisprudenza di legittimità, come abbiamo visto, non risulta applicabile a tutte le fattispecie criminose commesse nel cyberspace.

Molto dipende dalla struttura della fattispecie che di volta in volta viene in essere e dal momento consumativo. Molte le criticità avanzate nelle more di un intervento specifico destinato a placare le numerose problematiche delineate dall'orientamento delle Sezioni Unite. Alla luce di questo sarebbe auspicabile un intervento del legislatore, il cui obiettivo sia quello di recepire l'evoluzione dei principi tradizionali, in modo tale da consentire di valorizzare quelle particolari caratteristiche che assume il concetto di individuazione del locus commissi delicti nei cybercrimes.

Una recente sentenza della Cassazione[141] del 2020, ha offerto l'occasione, invece, per una rilettura complessiva della fattispecie di reato di cui all'art. 615 ter Cod. pen.

La Quinta Sezione, infatti, si è occupata del caso di un professionista, socio sia di uno studio professionale associato che di una società di professionisti, che aveva effettuato il backup dei dati dei clienti per intraprendere un'attività autonoma e diversa rispetto a quella per cui i dati stessi erano stati raccolti. Pertanto era stato querelato per il reato di cui all'art.

[141] Sent. Cass., Sezione V, n. 34296 del 2.10.2020, depositata il 22.12.2020.

615 ter Cod. pen. e condannato in entrambi i gradi di merito, ricorrendo, infine, per cassazione. In sede di legittimità, lamentava l'erronea applicazione dell'art. 615 ter Cod. pen. poiché l'accesso al sistema informatico sarebbe stato eseguito a seguito dell'utilizzo delle chiavi di cui era legittimamente in possesso e ribadendo come nessuna normativa interna all'associazione o alla società vietasse espressamente l'utilizzo per finalità con cui erano state impiegate.

La Corte ha respinto il ricorso affermando nuovamente il principio per cui vi è accesso abusivo a sistema informatico ogni volta che l'agente entri o si trattenga nel sistema per finalità diverse da quelle "istituzionalmente" previste per l'accesso.

Per il legislatore del 1993 che ha inserito l'art. 615 ter Cod. pen. tra i reati che tutelano l'inviolabilità del domicilio, il referente normativo di rango costituzionale era senza dubbio l'art. 14 Cost..

Il diritto alla protezione dei dati personali, quindi, è da considerarsi un diritto di libertà sancito espressamente dal diritto positivo sul piano sovrannazionale, con una piena copertura di carattere costituzionale ex art. 117 Cost., tutelato dai regolamenti europei ma anche da normative primarie interne che fanno propri i principi posti dal diritto dell'Unione europea.

La questione che ha avvinto la giurisprudenza di legittimità in modo costante, dal 2012[142] ad oggi, è la portata del concetto di abusività dell'accesso e, a parte le ipotesi più scontate di sottrazione delle chiavi d'accesso o di elusione dei sistemi di protezione informatica, dottrina e giurisprudenza hanno dovuto confrontarsi con la casistica di accessi effettuati da soggetti che legittimamente detenevano le chiavi ma che le hanno utilizzate per scopi diversi da quelli per cui erano state attribuite.

[142] Con la sentenza Casani del 17 febbraio 2012, n. 4694, le Sezioni Unte hanno affermato che la condotta penalmente rilevante ai sensi dell'art. 615 ter Cod. pen. consiste sia nell'accesso che nel mantenimento del soggetto abilitato che "*violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitare oggettivamente l'accesso*". Con la sentenza Savarese del settembre 2017, n. 41210, le Sezioni Unite hanno affrontato la questione della qualificazione giuridica dell'utilizzo, da parte di un cancelliere, del sistema informatico 'Re.Ge' utilizzato alla Procura della Repubblica, per verificare se vi fossero notitiae criminis in capo ad un conoscente.

2.3 Attacchi hacker e reati informatici: tra codice penale e regolamentazione UE

Le motivazioni che spingono verso questi crimini sono sostanzialmente le stesse degli illeciti civili e penali, solo che sono trasferite sul sistema informatico; può trattarsi di reati contro la persona (diffamazione, furto d'identità), contro il patrimonio (furti, estorsioni) o contro le istituzioni (interruzioni di servizio, spionaggio, controllo dei sistemi). I criminali informatici, ormai colpiscono soprattutto account di posta elettronica e social, portali di eCommerce, siti web di aziende e, sempre più quelli istituzionali. Le tecniche di attacco al momento più diffuse sono le truffe (es. phishing) e l'estorsione che confermano come il fine più comune del cybercrime sia la realizzazione di introiti attraverso attività di carattere illecito.

Nel settore informatico i procedimenti che hanno come oggetto reati di questo tipo sono piuttosto limitati poiché, in molti casi non vengono denunciati anche se oggi assistiamo ad un graduale cambiamento. Anzi, la denuncia molto spesso viene considerata un'ammissione di vulnerabilità del proprio sistema informatico, con il timore di conseguenze anche sul piano della credibilità dell'azienda stessa nei confronti dei clienti, come nel caso delle banche[143].

I dati personali, ormai, hanno acquisito una centralità impensabile fino a pochi anni fa. I nostri dati vengono oggi raccolti in modo continuativo e spesso anche subdolo da tanti apparecchi connessi da cui siamo circondati. Non più solo pc, telefoni mobili ma anche orologi, automobili, televisori ed elettrodomestici vari, dotati di sensori sempre più sofisticati e per questo sempre più "intelligenti". Tutti questi oggetti continueranno a scambiarsi reciprocamente le informazioni raccolte per fornirci servizi via via più

[143] Sul punto si veda G. DEZZANI, *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica, in La responsabilità amministrativa delle società e degli enti,* Rivista 231, 2010, pag.80.

personalizzati, avvolgendoci in una confortevole bolla costruita intorno alle nostre abitudini[144].

Altre finalità comunque rimarchevoli sono: l'intrusione in un sistema informatico a scopo di spionaggio (es. politico, industriale, militare), l'interruzione di servizio (es. attacchi Dos – Denial of Service, DDos – Distributed Denial of Service), la manipolazione e l'influenza esercitata sull'opinione pubblica (es. durante le consultazioni elettorali), il controllo di sistemi strategici o produttivi (es. nel caso di centrali elettriche, impianti di produzione).

Già dagli anni Duemila lo United States Department of Defense[145] aveva evidenziato come il crimine informatico avesse assunto forme che coinvolgono direttamente le strategie di politica globale. Oltre agli attacchi di massa che sfruttano le vulnerabilità dei software comuni, è stato rilevato un sensibile aumento di attacchi contro le infrastrutture critiche degli Stati passando così rapidamente dalla nozione di di cyber attack a quello di cyber war.

Una definizione del termine "Cyber War" è riconducibile a Carlo Jean, generale e scrittore esperto di strategia militare e di geopolitica che sostenendo che la «cyberwar include tutte le forme di attacco e di difesa nel cyberspazio», la definisce come un'estensione della guerra elettronica nei suoi aspetti sia offensivi (contromisure, intercettazioni, ecc.) sia difensivi (contro-contromisure, crittografia, firebreak, ossia sbarramenti per impedire l'accesso alle reti e alle banche dati) che va strettamente coordinata con essa. Le finalità possono essere sia politico-strategiche sia economiche. Per Jean, «in entrambi i settori, le reti informatiche agiscono come moltiplicatori e anche come generatori di potenza economica e militare. […] La cyberwar è estremamente dinamica, rapida e imprevedibile. Annulla il valore della distanza, del tempo e delle frontiere. Rende possibili sorprese strategiche, molto di più quanto esse siano possibili con gli strumenti

[144] R. SCIAUDONE, E. CARAVÀ, *Il codice della privacy*, Commento al D.LGS. 30 giugno 2003, n.196 e al D.LGS. 10 agosto 2018, n.101 alla luce del Regolamento (UE) 2016/679 (GDPR), Prefazione, Pacini giuridica, Pisa, 2019, p. XXI

[145] Il Dipartimento della Difesa degli Stati Uniti (United States Department of Defense), DoD o DOD, è un'articolazione civile del governo federale degli Stati Uniti d'America. Controlla le Forze armate statunitensi. Il suo quartier generale è il Pentagono.

hard. Può consentire a piccoli gruppi o ad individui singoli collegati in Rete di esprimere una grande potenza e di provocare danni disastrosi».[146].

Viviamo in un'epoca in cui da un concetto di guerra fondato su capitale umano ed armi fisiche si è passati ad una rappresentazione molto più ampia, non più legata ai territori o ai mezzi di distruzione bensì basata su minacce invisibili in grado di attaccare informazioni o dati con l'intento di colpire ed arrecare danno, produrre una sorta di "blackout" e dimostrare quanto la vittima sia risultata vulnerabile.

Il primo episodio di guerra informatica tra Nazioni a livello mondiale può essere fatto risalire al 2007 quando la Repubblica d'Estonia si rese protagonista di uno scontro di carattere politico con la Russia, dopo la decisione di rimuovere dal centro della città di Tallinn, la capitale, un monumento al valore militare che risaliva all'epoca dell'occupazione sovietica. A parte alcune proteste iniziali il fatto non generò azioni belliche convenzionali da parte della Russia ma il governo estone diventò bersaglio di una serie di attacchi informatici attraverso tecniche di Distributed Denial of Service (DDoS). Si trattò di un'interruzione di servizio dovuto ad un attacco diretto verso i sistemi informatici dell'istituzione fino a compromettere le attività ordinarie e straordinarie pubbliche e private, le infrastrutture critiche ed i relativi servizi. Una chiara dimostrazione di come un cyber attacco possa trasformarsi in un serio problema di sicurezza nazionale.

Nell'ultimo decennio è evidente l'evoluzione delle cyber minacce e come i malware vengano utilizzati alla stregua di vere e proprie armi a disposizione delle maggiori potenze mondiali. Si tratta di tecniche e strumenti di competizione tra Paesi, in grado di danneggiare servizi essenziali e sistemi informatici militari e industriali degli Stati.

La cyberwarfare, dunque, è una vera guerra cibernetica che racchiude tutte le attività di cybercrime messe in atto da uno Stato nei confronti di un altro Paese attraverso il cyber space. Una forma ben coordinata di guerra tecnologica, supportata da nazioni che la usano come uno strumento strategico, quasi indispensabile per la competizione e la loro affermazione a livello mondiale.

[146] C. JEAN, P. SAVONA, *Intelligence Economica*, Rubbettino, 2011, p.14.

Per Cyber attivismo, invece, si intende una nuova forma di resistenza "culturale e politica" portata avanti dagli hacker. Questo tipo di attività è spinta da motivi di natura socio-politica o per fini di protesta su particolari e specifiche tematiche. Gli strumenti di attacco maggiormente utilizzati, in questo caso, sono il Distributed Denial of Service (DDoS), la raccolta illecita di dati personali (mediante attacchi di tipo APT) e la diffusione di dati e informazioni di carattere riservato (i c.d. Data breach e Data leaks). Fa parte del cyber attivismo anche l'attività c.d. di defacing, o meglio l'intrusione non autorizzata nel sito web con modifica dei contenuti del sito.

Il concetto di cyberlaw, invece, è strettamente legato alla criminalizzazione di condotte illecite commesse sulla rete: «Laws, or a specific law, relating to Internet and computer offenses, especially fraud or copyright infringement» (Oxford Dictionary).

In questa ampia categoria della cyberlaw rientrano le fonti normative che disciplinano la sicurezza delle reti e dei sistemi di informazione che disciplinano il rapporto tra utenti del mondo digitale allo scopo di proteggere interessi di primaria importanza quali la personalità individuale, la riservatezza delle comunicazioni, la confidenzialità delle informazioni, i dati personali e il diritto d'autore.

Il Cyber spionaggio, infine, riguarda generalmente operazioni di intelligence con l'obiettivo di accedere a informazioni riservate, sensibili e strategiche. Il fenomeno ha comportato la revisione di interi processi e metodologie di acquisizione ed elaborazione delle informazioni, in funzione della pervasività e dell'utilizzo crescente delle tecnologie informatiche e di Internet[147].

Si tratta, in sostanza, di una forma di minaccia ampia e di intensità variabile. In genere, precede le altre forme di cyber crime determinando ingenti danni finanziari o di reputazione agli Stati e alle aziende colpite fino a generare la potenziale esclusione dal mercato. Le attività più diffuse vanno dalla raccolta di informazioni aziendali segrete, alle intercettazioni di comunicazioni telefoniche o telematiche per poter disporre in anticipo di informazioni riservate su altre nazioni ostili o anche alleate, in periodi di pace ma anche in tempo di guerra. In questo campo, un prezioso contributo è stato fornito dalla

[147] A. TETI, C*yber intelligence e cyber espionage come cambiano i servizi di intelligence nell'era del cyber spazio*, in «Gnosis», Rivista italiana di intelligence, 3/2013, pp. 95-121

Raccomandazione del Consiglio d'Europa del 13 settembre 1989[148] sulla criminalità informatica in cui sono menzionate le condotte di abuso che fino ad allora erano oggetto di attenzione da parte dei diversi Paesi, indicando quelle che occorre reprimere con l'arma della pena, anche con interventi legislativi ad hoc.

All'interno della Raccomandazione era stata elaborata una lista minima in cui erano riportate le principali condotte della criminalità informatica: il falso in documenti informatici, la frode informatica, il sabotaggio, il danneggiamento di dati, l'intercettazione di comunicazioni informatiche, l'accesso abusivo a un sistema informatico e la violazione dei diritti su un programma protetto Vi era, inoltre, una lista facoltativa di condotte, per le quali da un punto di vista sanzionatorio era stata lasciata ampia discrezionalità ai legislatori nazionali.

Il rapidissimo sviluppo della tecnologia aveva spinto il Consiglio d'Europa all'elaborazione della Convenzione sulla criminalità informatica, cd. Cybercrime che è stata stipulata a Budapest nel 2001 (23 novembre) ed è entrata in vigore nel 2004. Uno strumento più incisivo e vincolante rispetto alla Raccomandazione, visto che mirava ad armonizzare i vari ordinamenti penali sul piano sostanziale e processuale. La Convenzione, infatti, indica un oggetto necessario di incriminazione individuandolo nelle condotte di abuso che precedentemente erano ricondotte alla nozione di reato informatico, facendo una distinzione a seconda che lo strumento informatico sia oggetto oppure strumento di aggressione[149].

In un primo elenco rientrano le offese arrecate alla riservatezza, all'integrità e alla disponibilità dei dati e dei sistemi informatici (accesso abusivo al sistema, intercettazione di comunicazioni informatiche, danneggiamento dei dati, sabotaggio).

Il secondo gruppo è costituito da quelle condotte in cui il sistema informatico rappresenta lo strumento oppure costituisce il mezzo per commettere i reati tradizionali di falso e di truffa, ovvero la falsificazione di dati informatici e la frode informatica.

[148] Conseil de l'Europe, Recommandation n. R (89) 9, Strasbourg. Tale raccomandazione si apre con il riconoscimento dell'importanza di una risposta adeguata e rapida al nuovo fenomeno della criminalità informatica e con la considerazione che la criminalità informatica ha spesso un carattere transfrontaliero.

[149] C. PECORELLA, *Reati informatici*, in Enc. Dir., 2017, Annali, X, Milano p. 707 e ss.

A questi si aggiunge un gruppo in cui rientrano le violazioni del diritto d'autore sulle opere dell'ingegno e altre condotte come la pornografia infantile caratterizzate dall'uso del sistema informatico nella commissione del reato.

Il Consiglio d'Europa, pertanto, richiede agli Stati di predisporre delle sanzioni effettive, dissuasive e proporzionate, indicando, come necessaria la previsione di una concorrente responsabilità anche per le persone giuridiche nel caso in cui il reato fosse stato commesso nel loro interesse da un soggetto dotato di poteri di rappresentanza, gestione o controllo al suo interno, oppure che fosse causato dalla mancanza di controllo o sorveglianza su un soggetto sottoposto[150].

È pacifico tuttavia che il diritto penale ha come compito principale la tutela di beni giuridici e la prevenzione delle condotte offensive. Un sistema giuridico per essere armonico quindi, deve contenere distinte categorie di tutela, la loro graduazione e la riduzione al minimo della possibilità di duplicazione o di contraddittorietà dei precetti[151].

Il vero pilastro nel contrasto al cybercrime rimane la Convenzione di Budapest anche se sono intervenuti successivamente la direttiva Nis (2016/1148) attuata con d.lgs. n.65 del 2018 e il Regolamento generale sulla protezione dei dati personali (2016/679) che hanno dettato obblighi di compliance con sanzioni molto incisive agli operatori essenziali e alle imprese[152]. Il regolamento 2019/881, c.d. Cybersecurity Act, invece, nell'ambito della strategia nazionale per la sicurezza della rete e dei sistemi informativi definita dalla Direttiva NIS, ha avuto l'obiettivo di realizzare un quadro europeo per la certificazione della sicurezza informatica dei prodotti e dei servizi digitali, in base ad un modello di *security by design*, rafforzando il ruolo dell'ENISA.

---

[150] Nel nostro ordinamento questa esigenza è stata soddisfatta con la l. 18 marzo 2008 n.48 che, attraverso l'inserimento dell'art. 24 bis nel d.lgs. 231/2001 ha esteso la responsabilità degli enti, originariamente prevista solo per le ipotesi di frode informatica in danno dello Stato o di altri enti pubblici (art. 24), a quasi tutti i reati.

[151] F. R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in dir. Pen. proc., 2009, p. 639 e ss.; F. Modugno, Ordinamento giuridico, in Enc. Dir., XXX,1980, p. 678 e ss.

[152] L. D'AGOSTINO, L*a tutela penale dei dati personali nel riformato quadro normativo un primo commento al D Lgs.10 agosto 2018, n.101*, in Arch. pen. web, 2019, 1,18 ss

Ma vediamo cosa accade nel nostro ordinamento: l'introduzione di specifiche figure di reato informatico si deve alla legge del 23 dicembre 1993 n. 547[153], la prima vera normativa contro il cybercrime, con la quale si è assicurata la repressione di gran parte delle condotte menzionate e sono state modificate e integrate le norme del codice penale e del codice di procedura penale che si riferivano alla criminalità informatica.

La legge in questione ha affiancato alle norme tradizionali sulla truffa e sul danneggiamento la nuova fattispecie di frode informatica (ex art 640 ter c.p. contenuto all'interno del Titolo XIII "dei delitti contro il patrimonio", Capo II "dei delitti contro il patrimonio mediante frode").

Con tale provvedimento si pongono le basi per una reale lotta al crimine informatico con la suddivisione in quattro macrocategorie delle aree di intervento: frodi informatiche, falsificazioni, integrità dei dati e dei sistemi informatici, riservatezza dei dati e delle comunicazioni informatiche.

L'art. 640-ter c.p. recita: «Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante». ("Frode informatica").

[153] Legge 23 dicembre 1993 n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

Il decreto legge 14 agosto 2013, n. 93 (art. 9, co. I, lett. a)[154] convertito con modificazione con legge 15 ottobre 2013, n. 119 ha previsto, all'interno dell'art. 640-ter c.p., una nuova circostanza aggravante ad effetto speciale del delitto di frode informatica: *«La pena è della reclusione da due a sei anni e della multa da euro seicento a euro tremila se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*».

Art. 648-bis c.p. in materia di riciclaggio: «Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648».

È necessario ricordare che possiamo distinguere due diversi tipi di fattispecie penali, le prime, rientranti nel Codice della Privacy, sono denominate reati privacy propri, mentre le seconde, presenti nel Codice Penale, sono definibili come reati privacy impropri.

Nel primo caso il reato privacy è proprio, in quanto esplicitamente definito tale dal D. Lgs.196/2003 (Garante privacy), e dunque tutela la riservatezza come bene giuridico.

Nel secondo caso, scindibile in reati privacy impropri informatici e non informatici, il bene giuridico della riservatezza è presente, ma insieme ad ulteriori beni giuridici dello stesso valore costituzionale, dando vita a dei reati dal carattere plurioffensivo[155].

Parlando di regolamentazione comunitaria in materia di reati informatici il principale problema derivante dalla regolamentazione del crimine informatico appare proprio la sua

[154] F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93* (convertito con modificazioni dalla L. 15 ottobre 2013, n.119), in Cass. Pen., 2014, p. 1094 e ss.

[155] Alcuni autori sono contrari alla categoria dei reati plurioffensivi, cfr. A. PAGLIARO, *Bene giuridico e interpretazione della legge penale,* in Studi in onore di F. Antolisei, II, Milano, 1965, p.398.

"aterritorialità". Si pongono dunque problemi a livello investigativo, visto l'ampio terreno da monitorare, a livello processuale e sul piano penale. Emerge così la necessità di dotare l'Unione Europea di una normativa specifica che sappia armonizzare le varie disposizioni nazionali e rendere più omogeneo l'intervento sui computer crimes.

Esaminando nel dettaglio le diverse tipologie di attacchi informatici è possibile notare come questi sfruttino ogni vulnerabilità e l'accrescersi della complessità dei siti web e lo sviluppo più rapido delle tecnologie tende ad aumenta il rischio di attacchi nella rete. Questi attacchi, come vedremo di seguito, possono avvenire con diversi mezzi e con modalità che variano a seconda del fine con il quale vengono perpetrati.

2.3.1 Phishing e Pharming

Il termine phishing deriva dall'unione di due termini inglesi phreaking (tecnica usata negli anni Settanta per effettuare telefonate gratuitamente) e "fishing (furto di identità, negli anni Novanta serviva ad ottenere dati personali e credenziali di account finanziari) e richiama proprio la modalità con cui l'utente viene adescato e persuaso a cliccare sul link malevolo[156].

Il phishing che ha fatto la sua prima apparizione nel 2003 quando l'FBI americano lo ha definito come "the hottest and the most troubling new scam on the internet", può essere considerata come una tecnica fraudolenta per estorcere informazioni di carattere personale, abitudini nonché stili di vita.

Si tratta di una truffa realizzata a danno di un utente con l'obiettivo di impossessarsi delle credenziali di account di servizi online attraverso l'accesso ad e-mail personali e conti bancari. Gli utenti, ricevendo questo tipo di comunicazioni che solo apparentemente provengono da enti, istituzioni o società reali, vengono quindi spinti a collegarsi a pagine web o siti non autentici, anche se appaiono molto simili a quelli istituzionali.

[156] Oxford English Dictionary Online, *"phishing, n." OED Online, March 2006, Oxford University Press.*, su dictionary.oed.com.

Vengono indotti ad inserire le proprie credenziali per l'accesso ad aree riservate a servizi online, come ad esempio l'home banking, cliccando su form o sui link falsi elaborati dallo stesso phisher.

Sono messaggi fraudolenti che richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito, l'username o la password per accedere ad un determinato servizio o altro tipo di informazioni di carattere personale. Nella maggior parte dei casi la truffa è perpetrata attraverso messaggi di posta elettronica, ma vengono utilizzati anche altri mezzi quali, ad esempio, i messaggi sms.

L' iter criminis consiste in una iniziale raccolta dei dati dell'utente, alla quale consegue una ulteriore condotta realizzata interamente online.

Il phishing nel tempo è divenuto sempre più sofisticato, sia migliorando il testo delle email sia diventando più capzioso. Ci si riferisce alle tecniche di phishing mirato nelle quali i truffatori acquisiscono informazioni personali di dettaglio profilando la vittima in varie modalità, non ultimo l'utilizzo dei social network per carpire informazioni più specifiche fino a realizzare la truffa (c.d. spear phishing)[157].

Sostituire o acquisire un'identità nuova o di altri anche per scopi illeciti è divenuto estremamente facile. I dati sul c.d. furto d'identità digitale, oggi riconducibile al più vasto fenomeno globale del cybercrime, sono preoccupanti, essendo emersa la sussistenza di vere e proprie associazioni a delinquere, che si dedicano alla vendita e allo scambio dei dati personali altrui illecitamente acquisiti[158].

Il funzionamento della maggior parte dei servizi online è contraddistinto dal binomio costituito da un nome utente e una password la quale, solitamente, è conosciuta solo al soggetto e al sistema che conferma la dichiarazione di identità del nome utente, autorizzandolo all'accesso[159].

---

[157] F. DI RESTA, *La nuova "privacy europea*. *I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori*, G. Giappichelli Editore, 2018, p. 178.

[158] F. CAJANI, G. COSTABILE, G. MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008, p. 188.

[159] G. FLORA, *Il furto di identità*, in AA.VV., Sicurezza e privacy: dalla carta ai bit (a cura di COSTABILE), Esperta Edizioni, 2005, p. 237.

L'obiettivo, ossia carpire l'identità digitale, viene realizzato proprio nel momento in cui l'utente, indirizzato al server compromesso, o per mezzo di programmi quali keylogger o web trojan scaricati attraverso la navigazione o su istigazione delle mail, fornisce ingenuamente i propri dati.

Le fasi di un attacco di phishing si possono distinguere in sei momenti distinti: Planning, Setup, Attack, Collection, Fraud e Post Attack.

Nella prima fase 'Planning'[160] l'attaccante stabilisce chi colpire, cosa sottrarre, quale tecniche utilizzare e quali sono gli obiettivi della frode che intende mettere in atto; nella seconda, 'Setup', l'attaccante crea e configura i tools e i meccanismi per sferrare l'attacco, e si procura i contatti e le informazioni sulle potenziali vittime di cui ha bisogno; nella fase 'Attack' inizia a instaurare un contatto con le potenziali vittime attraverso email, chat, web site, malware. L'intento è quello di indurre le vittime potenziali a compiere azioni per estorcere le loro credenziali; è nella fase 'Collection' che l'attaccante realmente sottrae le credenziali delle vittime tramite web form e mail telefono (anche a mezzo di invio di SMS ai quali si chiede di rispondere) e malware. L'attaccante commercia, vende o usa direttamente le credenziali nella fase 'Fraud' per scopi fraudolenti con l'uso diretto delle credenziali ad esempio, per acquistare beni, rubare denaro dal conto della vittima, usare le credenziali per furto di identità o per riciclaggio di denaro. Infine, in 'Post Attack' disattiva i meccanismi, copre le tracce, verifica il successo dell'attacco, controlla le reazioni e molto spesso pianifica nuovi attacchi.

In Italia, attualmente non esiste una disciplina giuridica specifica che consideri il fenomeno in questione. Esistono tuttavia diverse norme nelle quali identificare le diverse fasi che caratterizzano il phishing.

Nella maggior parte degli attacchi la condotta può essere ricondotta alla fattispecie di cui all'art. 494 c p (sostituzione di persona) ma ciò non può darsi per scontato a causa delle peculiarità proprie dello spazio virtuale.

---

[160] R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, op.cit. p. 899.

Ad esempio quando la mail riporta segni distintivi di una società o di un ente non è possibile individuare in essi una sostituzione di persona fisica. L'utilizzo sui siti web di dati personali o credenziali d'autenticazione di un determinato soggetto per accedere ai servizi, quali ad esempio la gestione online del conto corrente bancario, non configurerebbe né la sostituzione di una persona né l'attribuzione di un falso nome, di un falso stato o meglio di una qualità specifica a cui la legge attribuisce effetti giuridici.

Potrebbe ravvisarsi invece una limitata possibilità di applicazione dell'art 494 c. p. solo nel caso in cui il messaggio contenga riferimenti ad una persona fisica attraverso la simulazione di un nome o di uno stato particolare come nel caso di una firma riportata in calce al messaggio.

L'email fraudolenta contiene spesso un collegamento ipertestuale ingannevole che rinvia a un sito clone, grazie al quale vengono sottratti i codici d'accesso della vittima. Le credenziali vengono poi utilizzate per accedere a caselle di posta o conti online, al fine di ottenere la disponibilità di somme di denaro. È' in quest'ultimo caso che può dirsi perfezionato il reato di truffa comune (art. 640 c p).

L'oggetto della condotta (cioè gli artifici e i raggiri posti in essere) è perfettamente integrato dalla condotta del reo che induce la persona offesa ad interagire con la banca di fiducia o con una nota società di e-commerce, di modo che la vittima venga indotta in errore e comunichi i propri dati.

In una nota sentenza del Tribunale di Milano (Trib. sez. VIII penale, 7 ottobre 2011, n. 11696/2011) si è affermato che la riproduzione di colori, marchi ed altre caratteristiche di siti realmente esistenti può essere considerata un artificio in senso penalistico.

Quando il phisher accede all'account della vittima senza aver nessun titolo ed eludendo le misure di autenticazione e identificazione per la tutela dei dati in esso contenuti, si configura una ipotesi di accesso abusivo in un sistema informatico o telematico (art 615 ter c p).

Il phisher carpendo i dati d'accesso della vittima, li utilizza nei rispettivi account intervenendo nei sistemi informatici, ad esempio della banca, senza aver alcun titolo. In questo caso il reato di frode informatica (art 640 ter c.p.) è commesso contro l'istituto di credito colpendo il suo sistema informatico.

Una pronuncia della Cassazione stabilisce che integra il reato di frode informatica e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice d'accesso fraudolentemente intercettato, penetri abusivamente nel sistema informatico altrui effettuando operazioni illecite per poterne trarre profitto per sé o per altri. (Cass. Pen., Sez II, 24 ottobre 2018, n 48553).

La Corte in questo caso non ha specificato i rapporti tra la truffa comune, il cui schema commissivo si chiude con la comunicazione dei codici di accesso e, la frode informatica, integrata dal prelievo delle somme dal conto online. Il concorso tra i due reati non pare tuttavia ammissibile per cui andrebbe rimodulato con il solo reato di truffa, che si consuma al momento della sottrazione/ottenimento delle somme in concorso con l'accesso abusivo a sistema informatico (art 640 e 615 ter c p).

L'uso di tecniche sempre più sofisticate ormai presenta il phishing come un fenomeno in continua evoluzione.

Tra le nuove forme troviamo il vishing o Voice Phishing (Voice over Internet Protocol). L'attacco del visher consiste nell'attivazione di un account VoIP e nell'avvio di un sistema di chiamata automatico per contattare le potenziali vittime e spingerle, attraverso una registrazione vocale, a comporre il numero telefonico di un call center apparentemente in grado di risolvere problemi o fornire comunicazioni urgenti sul proprio conto corrente bancario o sulla propria carta di credito, richiedendo l'inserimento di dati personali.

Associato al vishing è lo smishing, termine che deriva dalla sintesi delle parole sms short message service e phishing e sta ad indicare una tecnica finalizzata ad estorcere dati sensibili e finanziari via sms con un comune messaggio inviato al cellulare del malcapitato di turno che invita a collegarsi ad un sito web per usufruire di un'offerta o di un servizio (scaricare suonerie, giochi oppure immagini) e sollecitando a fornire i dati personali.

Pharming

Di natura simile al phishing è il c.d. pharming con cui condivide le finalità e anche tutta la fase preparatoria.

Fino alla realizzazione di pagine web contraffatte le due tecniche di attacco sembrano essere identiche, muta solo la modalità con cui si attirano le vittime potenziali. A differenza

di quanto avviene nel phishing, nel pharming non si inviano email di spam, ma si attaccano i server DNS (Domain Name System) diffusi nella rete, un sistema di nomi di dominio grazie al quale gli indirizzi di rete significativi per l'utente (ad es. europa.eu.int.) vengono tradotti in nomi in forma astratta (ad es. IP 147.67.36.18) e viceversa[161]. Questi server, in sostanza, vengono utilizzati per fornire ai computer la traduzione delle url in indirizzi IP. Con questa tecnica si tende a modificare la corrispondenza numerica del dominio digitato in modo tale che i server DNS decodifichino una corrispondenza numerica diversa da quella reale ed indirizzino l'utente ad una pagina molto simile a quella di riferimento.

L'attacco ai server è molto più complesso e articolato rispetto all'inoltro di spam ed ha come obiettivo quello di sostituire l'indirizzo IP originale con quello dei propri server. In questo caso l'iter criminis si articola in più azioni, commesse in tempi diversi. La prima può essere ricondotta alla frode informatica (art. 640-ter c.p.), in cui l'evento di profitto è costituito dal rilascio di informazioni personali da parte dell'utente. Il successivo accesso all'account personale sarà invece perseguibile come accesso abusivo a sistema informatico o telematico (art. 615-ter c.p.).

Il tentativo di frode informatica nel pharming, invece, sarà configurabile, qualora l'utente non si lasci ingannare e ometta di comunicare le informazioni di autenticazione che lo riguardano.

L'utente che tenta di connettersi per esigenze personali (non più dunque, su richieste pervenute sull'account mail) viene di fatto indirizzato sulla pagina contraffatta senza neppure accorgersene. Sicuramente questi attacchi risultano di difficile realizzazione, ma se portati a termine riescono con grande abilità a generare vittime anche tra gli utenti che possono sembrare più esperti.

[161] F. LISI, G. MURANO, A. NUZZOLO, *I reati informatici*, Maggioli editore, 2004, p.52.

2.3.2 Malware e Ransomware

Tra gli strumenti utilizzati per portare a termine un attacco informatico, uno dei mezzi più utilizzati è indubbiamente l'utilizzo di un malware o "software malevolo[162]". Proprio dalla sintesi dei termini "malicious" e software", deriva il termine che sta a significare letteralmente "programma malvagi" e indica un qualsiasi programma informatico in grado di danneggiare il funzionamento e la sicurezza del sistema operativo. Un programma viene installato sul pc, senza che l'utente lo sappia, con l'obiettivo di rendere il dispositivo vulnerabile ad altri attacchi. Questo genere di software cerca di invadere, danneggiare o disattivare computer, sistemi, reti e dispositivi mobili, spesso assumendo il diretto controllo delle operazioni.

Pur non danneggiando gli hardware fisici di un sistema o le attrezzature di rete, possono, in ogni caso, sottrarre, criptare o eliminare i dati, compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi forniscano alcuna autorizzazione. I più utilizzati sono Internet e gli account mail.

Esistono diverse tipologie di malware, a seconda della modalità e dei danni da essi procurati. Il malware si trasmette attraverso Internet, spesso tramite la posta elettronica o la semplice navigazione, e tra le varietà più diffuse figurano virus, trojan horse, keylogger, worm e backdoor. Nel dettaglio, esistono malware cosiddetti "poliformici" che cambiano continuamente forma, e malware "metamorfici", che alterano completamente il loro codice. Entrambi sono molto difficili da individuare, non danneggiano gli hardware fisici di un sistema, né le apparecchiature di rete, ma sono capaci di trafugare, criptare o eliminare i dati, modificare o danneggiare le funzioni fondamentali di un computer nonché spiare le attività svolte dagli utenti.

Vediamo nel dettaglio i principali: Virus, Worm, Trojan horse, Spyware, Adware, Keylogger, Ransomware, Logic bomb.

Il Virus, software o parti di essi, si installano all'interno di altri programmi che si replicano ogni volta che vengono eseguiti (es. all'avvio anche automatico del programma

[162] https://www.cybersecurity360.it/nuove-minacce/malware-cosa-sono-come-riconoscerli-e-come-rimuoverli/

infettato). È un programma malevolo che ha la capacità di infettare un computer che comunemente si riferisce alla categoria di malware, tuttavia esso ne rappresenta una sottocategoria. È un malware che necessita dell'interazione da parte dell'utente per essere eseguito ed è in grado di infettare solo un singolo host.

I Worm, entrano nei sistemi informatici, modificano il sistema operativo del dispositivo infettato per replicarsi attraverso la rete, per diffondere un altro tipo di malware. Si tratta di un componente software dannoso autonomo che si replica per diffondersi in altri pc. In genere un worm modifica il computer che ha infettato, in modo tale da venire eseguito ogni volta che si dà avvio alla macchina. Rimane in attività fino a quando il computer non viene spento oppure non si arresta il processo.

Il mezzo più comune utilizzato per la diffusione è la posta elettronica: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato agli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm utilizzano spesso tecniche di social engineering per indurre il destinatario ad aprire l'allegato. Alcuni worm sfruttano dei bug di client di posta molto diffusi per eseguirsi automaticamente al momento della visualizzazione del messaggio e-mail.

Il Trojan horse, invece è un software che all'interno contiene istruzioni dannose finalizzate a far prendere il controllo del dispositivo dai criminali informatici ad insaputa degli utenti. E' un malware che si presenta come un software utile e apparentemente sicuro che l'utente esegue di sua spontanea volontà ma che in realtà contiene un codice dannoso che crea delle backdoor[163] in un sistema e generalmente arriva a causare la perdita o il furto di dati. Questo virus non è quindi in grado di replicare sé stesso ma richiede un'azione diretta dell'aggressore per far giungere il software maligno alla vittima che deve eseguire il file malevolo. Spesso i veicoli utilizzati per iniettare ed installare i Trojan horse sui sistemi sono i worm.

[163] Una backdoor (dall' inglese porta di servizio o porta sul retro) è un metodo, spesso segreto, per bypassare la normale autenticazione in un prodotto, un sistema informatico, un crittosistema o un algoritmo. Spesso è scritta in linguaggi di programmazione diversi per superare le difese imposte da un sistema, come può essere un firewall, per accedere da remoto ad un pc, ottenendo attraverso un sistema di crittografia un'autenticazione che permetta di prendere il completo o parziale possesso del computer vittima.

I Spyware, servono per raccogliere e trasmettere all'esterno informazioni sul dispositivo infettato e sull'utente che lo utilizza come ad esempio credenziali e password) a sua insaputa, sfruttando le consuete tecniche di ingegneria sociale. Consente di raccogliere informazioni su una persona o un'organizzazione senza che questi se ne accorgano; può monitorare e registrare l'attività eseguita su un sistema di destinazione, ad esempio registrare le pressioni dei tasti (è il caso anche di malware detti Keylogger), o raccogliere le informazioni su carte di credito e di altro tipo. Molti programmi open source su internet nascondono in realtà un malware di questo tipo: il software dunque non è gratuito, ma viene pagato attraverso un'invasione della privacy dell'utente, spesso inconsapevole. In alcuni casi, la stessa applicazione che promette di liberare dagli spyware ne ha in realtà installato uno o è essa stessa uno spyware. Alcuni attacchi possono prevedere l'utilizzo di più malware contemporaneamente come nel caso di una botnet. Quest'ultima è una o rete di bot (detta anche armata zombi) composta da un gran numero di computer dirottati da malware al fine di raggiungere l'obiettivo prestabilito del criminale informatico che l'ha ideata. Vengono generalmente utilizzate per inviare spam o virus, rubare i dati personali o lanciare attacchi DDoS attraverso il controllo di centinaia o migliaia di computer.

I malware che orientano la navigazione dell'utente su siti pericolosi e visualizzano pagine e pop up, annunci pubblicitari anche fraudolenti sono chiamati Adware. Keylogger è invece un malware che, una volta installati sul dispositivo infettato e memorizzano tutto ciò che l'utente digita sulla tastiera e lo trasmettono all'esterno senza che risulti un malfunzionamento evidente.

Il ransomware, è un software che cripta tutti i dati presenti in memoria (dischi) o sulla rete locale del dispositivo infettato e li rende non più utilizzabili se non con il pagamento di un riscatto. Infine i Logic Bomb, sono quei programmi che funzionano appunto come bombe ad orologeria[164], utilizzano un codice malevolo celato nell'applicazione, eseguito solo al verificarsi di un evento. Un esempio è dato dalle "Time Bomb" che attivano il malware dopo un certo periodo di tempo al fine di restare silenti e propagarsi in altri dispositivi prima di essere riconosciuti.

[164] G. AMATO, V.S. DESTITO, G. DEZZANI, C. SANTORIELLO, *I reati informatici*, op. cit. p.101

Il ransomware

Con il termine ransomware è indicata una categoria di malware che, una volta installati, rendono inaccessibili i dati dei computer infettati e chiedono il pagamento di un riscatto per poterli ripristinare[165].

Alcune forme bloccano il sistema e intimano l'utente a pagare per poterlo sbloccare, altri invece cifrano i file dell'utente chiedendo una somma di denaro per riportare i file cifrati in chiaro (i virus di questo tipo sono detti Crypto).

I vettori d'infezione più comunemente utilizzati dai ransomware sono le e-mail di phishing, il cosiddetto "driven by download" ("scaricamento ad insaputa").

Ad esempio, appaiono sotto forma di banner pubblicitari sui quali invitano l'utente a cliccare per poi far gravare sul dispositivo il ransomware: in questi casi si parla di "Adware", ovvero malware da pubblicità, dal termine inglese advertisement.

Sia che si tratti di un pc, di un server, di un tablet, di uno smartphone o di qualsiasi tipo di dispositivo Internet of Things, i dati dell'utente vittima dell'operazione verranno presi in ostaggio fino a quando il proprietario del dispositivo non pagherà il riscatto per rimuovere la restrizione. Il ransomware colpisce individui, settore pubblico, aziende e piccole e medie imprese. Gli eventi recenti hanno acceso i riflettori su questo fenomeno e si prevede che le minacce ransomware continueranno a crescere.

Inizialmente diffusi in Russia, gli attacchi con ransomware sono ora perpetrati in tutto il mondo.

Nel panorama delle minacce informatiche e degli attacchi hacker, i ransomware sono considerati tra i più pericolosi e più diffusi, come testimoniano molti casi recenti che esamineremo più avanti, perché in grado di arrivare ai sistemi centrali di aziende e istituzioni, bloccarli dall'interno e addirittura paralizzarne l'attività. Sul monitor della vittima compaiono, nella maggior parte dei casi, istruzioni molto dettagliate e ben articolate per finalizzare la transazione in tempi stabiliti. Le indicazioni riportate sono in italiano

[165] https://www.cybersecurity360.it/nuove-minacce/ransomware/attacchi-ransomware-quali-rischi-per-le-aziende-come-affrontarli-e-come-difendersi/

corretto e consentono di pagare il riscatto mediante la TOR network[166], anche nota come DarkWeb. TOR (acronimo di The Onion Browser), ossia il browser a cipolla indica un metodo di comunicazione in rete che si basa sull'anonimato.

TOR pur essendo molto utile per fini legittimi, può rivelarsi altrettanto pericoloso, ed è spesso utilizzato nel caso delle richieste di riscatto che seguono un attacco ransomware. Attraverso questo meccanismo è praticamente impossibile risalire all'identità di chi invia i messaggi e gestisce le transazioni. E poiché il pagamento del riscatto dovrà avvenire nelle modalità stabilite, le organizzazioni che predispongono gli attacchi ransomware istituiscono dei veri e propri customer care, disponibili via chat.

Dopo il versamento del denaro, ove avvenga la vittima riceve una password che consente di sbloccare i files presi in ostaggio. Prevenire il ransomware è possibile attraverso una soluzione anti-malware che blocca i messaggi dannosi.

2.3.3 Dos e DDos e altre tipologie

Il termine *DoS (Denial of Service*)[167] sta ad indicare un'interruzione di servizio causato da un attacco informatico in cui si colpiscono deliberatamente le risorse di un sistema informatico che fornisce un servizio ai clienti, ad esempio un sito web o un web server, fino a renderlo non più in grado di erogare il servizio. Una versione più aggressiva è il DDoS: l'obiettivo è quello di colpire mediante un sovraccarico di traffico proveniente, a differenza del più semplice DoS, da fonti diverse. La tecnica è molto diffusa poiché le probabilità di successo è molto alta. Gli attacchi provengono da numerose fonti dislocate di

[166] Tor (The Onion Router): si tratta di un programma freeware realizzato da Tor project che consente agli utenti di navigare in maniera anonima e con la massima sicurezza. Si tratta di un software libero, rilasciato su licenza BSD, con un'interfaccia di gestione disponibile (Vidalia), basata sulla seconda generazione del protocollo di rete di onion routing. Con il suo utilizzo è molto più difficile tracciare l'attività Internet dell'utente essendo finalizzato a proteggere la privacy, senza che le comunicazioni confidenziali vengano monitorate o intercettate. È disponibile per Windows, Android e diversi sistemi operativi unix-like (compresi Linux e MacOS), soprattutto tramite le distribuzioni Lightweight Portable Security.

[167] https://cert-agid.gov.it/glossario/ddos-dos/

difficile localizzazione. A causa di un traffico troppo elevato i server vengono spenti e la conseguenza è l'interruzione del servizio.

Altre tipologie di attacchi informatici, ognuna con precise caratteristiche, differenti obiettivi e uno specifico scenario tecnologico sono: gli attacchi tramite cookie, SQL Injection, Sniffing, Doxing e attacchi personali.

Gli attacchi tramite *cookie* sono dei piccoli file di testo inviati da un sito al computer dell'utente che lo visita. Si tratta di file innocui, che hanno come unico obiettivo quello di identificare l'utente e di eseguirne la profilazione. Questi possono essere impiegati da un hacker che può sfruttare alcune vulnerabilità dei siti per intercettare questi cookie e utilizzarli per impersonare l'utente: potrebbe così anche riuscire ad appropriarsi di account e credenziali di accesso, senza che né l'utente né il sito se ne accorgano.

SQL Injection, invece, rappresenta una tecnica di code injection, usata per attaccare applicazioni di gestione dati e siti Web, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che queste ultime vengano poi eseguite automaticamente. In base al codice inserito, un hacker può avere accesso a diverse informazioni, tra cui le credenziali di accesso oppure, può permettere l'invio del contenuto del database all'insaputa della vittima.

Con la tecnica *Sniffing* malintenzionati esperti possono inserirsi in una rete locale per catturarne il traffico ad esempio, ai danni di una rete wi-fi casalinga poco protetta.

Un sistema poco sofisticato ma comunque molto efficace è quello *Doxing* per impossessarsi di informazioni personali che utilizza metodi non automatici, a volte anche semplicemente chiedendoli con l'inganno ai diretti interessati o effettuando ricerche incrociate sul web.

Le tecniche di attacco fin qui elencate possono essere utilizzate singolarmente o in maniera associata e si diffondono in modi differenti.

Dunque, alcuni reati informatici, come gli attacchi DDoS, hanno l'obiettivo di creare disagio all'azienda e produrre un'interruzione nell'erogazione del servizio.

La maggior parte degli attacchi ha però un altro scopo altrettanto grave e più pericoloso: il furto di dati. In attacchi a società finanziarie sono rubate informazioni quali

numeri di previdenza sociale, numeri di conto e informazioni bancarie, mentre per quelle che operano nel settore dei social media i dati che interessano sono quelli su attitudini e interessi dei clienti.

Le informazioni che sono state sottratte tramite, solitamente, data breach vengono messe in vendita sul mercato nero, il dark web, sul quale i venditori offrono "pacchetti" di dati tra cui gli acquirenti possono scegliere a seconda della tipologia. Il prezzo dei dati varia a seconda delle informazioni che contengono e a seconda del paese.

La vendita sul mercato nero tuttavia non è l'unico fine degli attacchi che mirano ad un data breach. Basti pensare al potenziale economico che le informazioni sulla salute dei pazienti potrebbero avere, una base dati su cui effettuare studi per calcolare i prezzi delle assicurazioni o per lo sviluppo di nuovi farmaci.

In Europa, con l'entrata in vigore nel 2018 del Regolamento generale sulla Protezione dei dati, è stato introdotto, in caso di violazione, l'obbligo per il titolare del trattamento di notifica all'autorità competente, con la descrizione della natura della violazione dei dati personali compromessi, le categorie e il numero indicativo di interessati coinvolti nonché le categorie e il numero di registrazioni dei dati personali.

Qualora la violazione sia tale da compromettere i diritti e le libertà di persone fisiche, il Regolamento prevede l'obbligo di notifica anche all'interessato senza ritardo.

L'introduzione da parte dell'Unione europea e delle amministrazioni mondiali di norme destinate alla divulgazione di casi di reati informatici testimonia l'interesse mondiale nel garantire trasparenza tra le imprese e nei confronti dei cittadini.

2.4 Il contrasto al cyberterrorismo: la direttiva 2017/541 UE contro le organizzazioni criminali strutturate

La Direttiva (UE) 2017/541[168] del Parlamento europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo rappresenta il nuovo passo compiuto dal legislatore europeo nella prospettiva del contrasto al terrorismo internazionale, per colmare le lacune di tutela esistenti e migliorare il sistema giuridico eurounitario.

La Direttiva rinviene il suo fondamento nell'art. 83, par. 1, TFUE[169] ed è il risultato di un lungo processo negoziale volto ad aggiornare e rafforzare il quadro giuridico europeo – precedentemente definito dalle Decisioni Quadro 2002/475/GAI [170] e 2008/919/GAI [171] - alla luce della Risoluzione 2178 (2014), del Protocollo Addizionale alla Convenzione del Consiglio d´Europa per la prevenzione del terrorismo del 2015[172] e della quinta raccomandazione del Gruppo di Azione Finanziaria Internazionale del 2012 (FATF/GAFI)[173] .

[168] Direttiva (UE) 2017/541 ha di fatto sostituito la Decisione quadro 2002/475/GAI e modificato la Decisione 2005/671/GAI del Consiglio.

[169] L'art. 83, par.1, TFUE prescrive che «*Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni*». Il terrorismo costituisce la prima sfera di criminalità che il legislatore europeo ha inteso contemplare nell'elenco tassativo contenuto nel successivo comma.

[170] Decisione Quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo, GUUE L 164, 22.6.2002, p. 3 (non più in vigore).

[171] Decisione Quadro 2008/919/GAI del Consiglio, del 28 novembre 2008, che modifica la Decisione Quadro 2002/475/GAI sulla lotta contro il terrorismo, GUUE L 330, 9.12.2008, p. 21 (non più in vigore).

[172] Consiglio d'Europa, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, CETS n. 217.

[173] Le Raccomandazioni FATF/GAFI del 2012, disponibili all'indirizzo web: http://www.fatfgafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

Partendo dalla definizione contenuta nell'art 270 sexies c. p.: «*Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia*»[174].

Le caratteristiche intrinseche del cyberspace offrono enormi potenzialità di finanziamento delle associazioni terroristiche, delocalizzando e globalizzando anche fenomeni circoscritti da un punto di vista territoriale. Del resto, all'indomani degli attentati dell'11 settembre 2001, il problema della sicurezza cominciò ad espandersi senza mai cessare del tutto, nonostante i provvedimenti adottati nei vari Paesi per migliorare la capacità di controllo e di prevenzione finalizzata alla sicurezza dei cittadini[175].

La nozione di cyber terrorismo può quindi ricomprendere due distinte tipologie di condotte: quelle target oriented dove la rete rappresenta lo strumento per il compimento dell'atto terroristico e quelle tool oriented in cui Internet diviene un mezzo di supporto per la diffusione del credo terroristico.

Dunque, l'uso di Internet oggi per le organizzazioni terroristiche o i singoli terroristi assume diversi scopi: o per danneggiare o compromettere i sistemi informatici o le infrastrutture critiche di un dato Paese o per svolgere tutte le attività inerenti alla gestione e alla sopravvivenza dell'organizzazione terroristica, quali azione di propaganda, raccolta fondi, comunicazione e reclutamento.

[174] Si tratta di una clausola di chiusura c.d. in bianco, poiché consente l'automatico adeguamento dell'ordinamento italiano alle possibili ulteriori definizioni che possono essere elaborate da norma internazionali vincolanti per l'Italia.

[175] M. IASELLI, *Manuale operativo del D.P.O. (Data Protection Officer)*, Maggiol, Rimini, 2018, p.5.

L’esigenza di intervenire sulla materia era già stata sottolineata nella risoluzione del Parlamento europeo del febbraio 2015 adottata a seguito degli attentati alla sede parigina della rivista satirica di Charlie Hebdo del 7 gennaio 2015[176].

La nuova disposizione rientra negli interventi di modifica/revisione/sostituzione degli atti dell’Unione dell’ex terzo pilastro, sulla scorta di quanto richiesto al Parlamento europeo, al Consiglio e alla Commissione dalla dichiarazione n. 50 allegata all’atto finale della conferenza intergovernativa che ha adottato il Trattato di Lisbona.

La direttiva 2017/541/UE, dunque, in virtù dei poteri concessi a Parlamento europeo e Consiglio dall’art. 83, par. 1 TFUE, si prepara ad ampliare il novero dei reati terroristici, connessi e riconducibili ad un gruppo terroristico, intervenendo anche nel caso di concorso, istigazione e tentativo.

Le sfide più urgenti negli ultimi anni derivano, soprattutto, dalla peculiarità del terrorismo internazionale di matrice jihadista che si distingue per le strutture decentralizzate che lo caratterizzano, capaci di operare in rete anche a notevole distanza grazie all’abilità nell’uso di nuove tecnologie informatiche. Strutture capaci di mobilitare quelle che vengono definite le “vocazioni” di singoli individui che seguono il programma criminoso del gruppo facendo ricorso ad armi rudimentali, molto spesso improvvisate ed imprevedibili.

Una minaccia pervasiva che richiede strategie di contrasto nuove, sia sul piano del diritto sostanziale che sul piano della cooperazione internazionale. Il terrorismo prende a bersaglio beni giuridici primari (quali la vita, l’integrità fisica delle persone, le strutture politiche, costituzionali, economiche e sociali) la cui tutela esige una anticipazione dell’intervento penale che deve comunque sempre mantenersi nell’alveo del rispetto dei principi generali del diritto penale e dei diritti fondamentali.

Le iniziative legislative europee degli ultimi anni sono state avviate sotto la pressione di questa emergenza dettata dagli attacchi terroristici, proprio come è avvenuto in passato per l’adozione della nostra legislazione nazionale antimafia. Tuttavia non può essere

[176] L'attentato terroristico alla sede del giornale satirico Charlie Hebdo è avvenuto il 7 gennaio 2015 a Parigi. Fu rivendicato dalla branca yemenita di Al-Qāʿida (o Ansar al-Sharia), Furono assassinate dodici persone, mentre undici rimasero ferite.

definita come una "legislazione emergenziale" o derogatoria dei principi fondamentali. Si tratta di un sistema normativo che mira ad affrontare il fenomeno criminoso in tutti i suoi aspetti.

La Direttiva sulla lotta al terrorismo offre un quadro organico sugli obblighi di incriminazione dei fatti di terrorismo, individua nuove fattispecie, con particolare attenzione alla prevenzione, allo scambio di informazioni ma anche all'utilizzo di strumenti già previsti per la criminalità organizzata e dedica infine, uno spazio specifico alla tutela delle vittime.

Si è arrivati quindi a nuove fattispecie di reato non contemplate dalle Decisioni Quadro ma ritenute fondamentali per contrastare le nuove minacce costituite dai cd. "lupi solitari" e dal fenomeno dei "foreign fighters[177]".

La principale fonte di preoccupazione è rappresentata dai c.d. foreign fighters spesso nati negli stessi paesi occidentali, che si recano in zone di conflitto, Siria e Iraq specialmente, per unirsi ai gruppi terroristici o per essere addestrati con lo scopo di acquisire un'esperienza operativa che possa consentire loro di perpetrare, al loro ritorno in Europa, attività di radicalizzazione e reclutamento e nuovi attacchi criminali.

Una definizione di foreign terrorist fighters si può trovarenella Risoluzione ONU n. 2178/2014[178] che li descrive «*individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*».

[177] S. KRAEHENMANN, '*Foreign Fighters under International Law*', Academy Briefing No 7, Geneva Academy of International Humanitarian Law and Human Rights, October 2014, p. 5-6

[178] La risoluzione 2178(2014) del Consiglio di sicurezza dell'ONU sui combattenti terroristi stranieri, La Risoluzione ONU introduce, al par. 6, l'obbligo per tutti gli Stati membri delle Nazioni Unite di criminalizzare quei comportamenti che potrebbero essere collegati o correlati al fenomeno dei foreign fighters. È stato infatti riconosciuto che il terrorismo non può essere sconfitto con la sola forza militare, le misure di contrasto e le operazioni di intelligence, ma è necessario considerare le condizioni che favoriscono la diffusione del terrorismo, dal piano della repressione a quello della prevenzione.

Ma vediamo i dati ufficiali che testimoniano un fenomeno in crescita[179]. 436 attacchi terroristici, compresi quelli falliti e sventati, sono stati registrati nei paesi dell'Unione Europea dal 2017 al 2019 (erano 895 nel periodo 2014-2017). Il 63% sono riconducibili a gruppi separatisti ed etno-nazionalisti, il 16% a movimenti della sinistra radicale, il 2,8% a gruppi di estrema destra (in diminuzione nel 2019 ma in aumento nel 2020). Il 18% è costituito da azioni di matrice jihadista. Pur essendo una parte marginale, gli atti riconducibili al jihadismo, sono causa di tutte le morti per terrorismo nel 2019 e di 16 uccisioni nel 2020.

L'onda lunga del terrorismo in Europa, emerso con il fenomeno Stato islamico a partire dal 2014, ha fatto registrare 146 azioni in nome del jihad dal 2014 al 2020: vi hanno preso parte 188 terroristi, dei quali 59 sono morti in azione. I morti sono 406 e 2.421 i feriti (database START InSight[180]). Nel 2020 gli eventi riconducibili alla violenza jihadista sono stati 25, contro i 19 dell'anno precedente e con un raddoppio di azioni di tipo "emulativo", ossia ispirate da altri attacchi portati a compimento nei giorni precedenti. Nel 2020 sono il 48% del totale le azioni emulative; erano il 21% nel 2019. Il 2020 ha fatto registrare inoltre, una progressiva diminuzione di azioni strutturate e coordinate che, con il tempo, hanno ceduto ad azioni individuali, non organizzate, spesso improvvisate e fallimentari[181].

A questi si aggiungono i c.d. lupi solitari ossia gli estremisti[182] che operano isolatamente negli stessi paesi occidentali in cui vivono. Si organizzano in maniera autonoma oppure in piccoli gruppi destrutturati, al di fuori delle associazioni terroristiche e, dopo aver acquisito informazioni utili sull'uso di armi o esplosivi, generalmente attraverso il web, si attivano per compiere attentati.

---

179 C. BERTOLOTTI, *Immigrazione e terrorismo. I legami tra flussi migratori e terrorismo di matrice jihadista,* Lugano, 2020.

180 START InSight è una casa editrice della Svizzera italiana specializzata nella saggistica su argomenti legati all'analisi politica, strategica, sociale e delle conflittualità a livello globale, con particolare attenzione alle aree europea, mediterranea e del Medioriente allargato.

181 C.BERTOLOTTI, I*l terrorismo in Europa, Francia Germania e Italia: tra attacchi, contrasto ed espulsioni*, Trimestrale società italiana per l'organizzazione internazionale. Nuove forme di estremismo: strumenti di prevenzione e contrasto delle minacce, Editoriale Scientifica, p.13.

182 https://www.interno.gov.it/it/notizie/contro-terrorismo-attenzione-foreign-fighter-e-lupi-solitari

E' bene tuttavia segnalare come la normativa italiana, dopo le modifiche intervenute con il d.l. 7/2015[183] (conv. l. 43 del 2015) e la l. 153/2016[184], risultava già in linea con i nuovi obblighi di incriminazione europea, dei quali, anzi, si potrebbe dire sia stata anticipatrice.

Le principali novità si registrano nell'ambito dei reati connessi alle attività terroristiche, attraverso l'imposizione di obblighi specifici in capo agli Stati membri affinché vengano qualificati come reato: ricevere addestramento a fini terroristici (art. 8); viaggiare a scopi terroristici, sia all'interno che all'esterno dell'Unione europea (art. 9); finanziare, facilitare o organizzare tali viaggi (art. 10); apportare fondi per la commissione di reati terroristici (art. 11).

Si ribadisce la necessità che sia punita come reato «se compiuta intenzionalmente, la diffusione o qualunque altra forma di pubblica divulgazione di un messaggio, con qualsiasi mezzo, sia online che offline, con l'intento di istigare alla commissione di

uno dei reati di terrorismo, se tale comportamento, direttamente o indirettamente ad esempio mediante l'apologia di atti terroristici, promuova il compi mento di reati di terrorismo, creando in tal modo il pericolo che uno o più di tali reati possano essere commessi» (art 5).

Si precisa, inoltre, che i reati riconducibili alla «pubblica provocazione per commettere reati di terrorismo » comprendono « l'apologia e la giustificazione del terrorismo o la diffusione online e offline di messaggi o immagini, comprese quelle riguardanti le vittime del terrorismo, quale mezzo per raccogliere sostegno alle cause dei terroristi o intimidire gravemente la popolazione » e che «per ogni caso concreto,

[183] D.L. 18 febbraio 2015, n. 7 "*Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione".* Entrata in vigore del provvedimento: 20/02/2015, ad eccezione dell'art. 15, commi 6-bis e 6-ter che entra in vigore il 1/06/2015. Decreto-Legge convertito con modificazioni dalla L. 17 aprile 2015, n. 43 (in G.U. 20/04/2015, n. 91).

[184] L. 28 luglio 2016, n. 153- Norme per il contrasto al terrorismo, nonché ratifica ed esecuzione di convenzioni internazionali in materia (GU 9.8.2016).

nell'esaminare se sussista un siffatto pericolo, si dovrebbe tenere conto delle specifiche circostanze del caso, come l'autore e il destinatario del messaggio, nonché del contesto in cui l'atto è commesso tenuto conto altresì dell'entità e della natura verosimile del pericolo» (v considerando 10).

L'intento repressivo è quello di punire il soggetto appartenente all'organizzazione terroristica come figura apicale o semplice partecipante ma anche colui che contribuisca consapevolmente alla commissione di reati terroristici anche se esterno all'organizzazione.

Agli Stati membri è imposta, inoltre, l'adozione di sanzioni penali effettive, proporzionate e dissuasive per punire i reati individuati dalla direttiva.

Per i delitti di cui all'art. 3, par. 1 (reati di terrorismo) e all'art. 14 (concorso, istigazione e tentativo), si richiedono pene detentive più severe rispetto a quanto previsto dal diritto nazionale per i corrispondenti reati comuni in assenza della finalità di terrorismo.

Come già previsto dalla precedente decisione quadro 2002/475/GAI, così come modificata dalla decisione quadro 2008/919/GAI, la pena della reclusione è non inferiore nel massimo ad anni quindici per la condotta di direzione di un'organizzazione terroristica e non inferiore ad anni otto per le attività di partecipazione alle attività illecite.

La reclusione non inferiore nel massimo ad anni otto si applica anche nel caso in cui il soggetto posto a direzione di un'organizzazione terroristica minacci di commettere uno dei reati terroristici di cui all'art. 3, par. 1 della direttiva (art. 15).

Per la prima volta si obbligano gli Stati membri ad adottare le misure necessarie per assicurare la rimozione urgente dei contenuti online ospitati nel loro territorio che rappresentano una pubblica provocazione per commettere un reato di terrorismo come indicato all'articolo 5 e di adoperarsi per la rimozione anche nel caso in cui i contenuti siano ospitati al di fuori del loro territorio (art.21).

Qualora non fosse possibile rimuoverli alla fonte, è introdotto l'obbligo di adottare misure idonee per bloccare l'accesso a questi contenuti agli utenti Internet sul loro territorio.

La Commissione europea con la Comunicazione del 21 settembre 2005[185] aveva già affrontato il tema della radicalizzazione, definendola quale «fenomeno che vede persone abbracciare opinioni, vedute e idee che potrebbero portare ad atti terroristici quali definiti all'articolo 1 della Decisione quadro del 2002 sulla lotta contro il terrorismo». Da qui si poteva evincere la consapevolezza che lo strumento penale da solo non può essere sufficiente a debellare il "virus" del fondamentalismo ma sarebbe stato necessario intervenire prima su settori strategici come l'istruzione e la partecipazione dei giovani alla vita sociale, l'inclusione e l'integrazione, l'uguaglianza di opportunità e il dialogo interculturale.

Non a caso, la Commissione con la Comunicazione del 15 gennaio 2014[186], a proposito di prevenzione e radicalizzazione, ha fissato un decalogo di priorità per gli Stati membri che privilegia l'elaborazione di strategie nazionali, la valorizzazione della Rete per sensibilizzare in materia di contrasto alla radicalizzazione (RAN) e condivide l'ortoprassi, la formazione degli operatori che lavorano a contatto diretto con individui esposti al rischio di radicalizzazione, nonché lo sviluppo delle tecniche di contronarrativa[187].

Col dilagare del fenomeno dei foreign fighters e del c.d. terrorismo spontaneista, l'Agenda europea sulla sicurezza 2015-2020[188] ha contemplato poi, tra le tre priorità per la sicurezza nello spazio euro-unitario, proprio la lotta al terrorismo e la prevenzione della

[185] Comunicazione della Commissione al Parlamento europeo e al Consiglio del 21 settembre 2005 (COM (2005) 313 definitivo) «*Reclutamento per attività terroristiche – affrontare i fattori che contribuiscono alla radicalizzazione violenta*».

[186] Comunicazione della Commissione al Parlamento europea, al Consiglio, al Comitato economico e sociale e al Comitato delle Regione del 15 gennaio 2014 (COM (2013) 941 definitivo) «*prevenire la radicalizzazione che porta al terrorismo e all'estremismo violento: rafforzare la risposta dell'UE*».

[187] Il termine storytelling (o narrativa) per indicare il complesso di basi ideologiche e atti comunicativi adottati dai gruppi estremisti per mantenere la coesione interna, indicare in modo chiaro i propri obiettivi soprattutto alle cellule indipendenti, pubblicizzare la propria causa, reclutare nuovi membri e dare uno scopo e una coerenza di fondo alle proprie attività.

[188] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regione del 28 aprile 2014 (COM (2015) 185 definitivo) «*Agenda europea sulla sicurezza*». L'Agenda ha fornito un quadro chiaro per una migliore collaborazione in materia di sicurezza nella UE e ha posto le basi per una rinnovata strategia di sicurezza interna da parte del Consiglio europeo.

radicalizzazione jihadista. Gli altri due fattori di rischio sono la criminalità organizzata transfrontaliera e quella informatica.

Ulteriori disposizioni sono introdotte in materia di confisca (art. 20), al fine di coordinare l'azione repressiva in materia di terrorismo con la disciplina di cui alla direttiva 2014/42/UE in materia di congelamento e confisca dei beni strumentali e dei proventi da reato, e in materia di contrasto ai contenuti online riconducibili alla pubblica provocazione a commettere reati terroristici (art. 21).

La direttiva dedica infine il titolo V alle disposizioni in materia di diritti, protezione e sostegno alle vittime del terrorismo, tra cui vengono ricomprese non solo la persona offesa e il danneggiato dal reato, ma anche il familiare di una persona deceduta in conseguenza di un attentato terroristico. Il titolo prende in considerazione i soli reati terroristici di cui all'art. 3 della direttiva, consistendo gli altri delitti in condotte preparatorie che, di regola, non mietono vittime dirette.

Spicca l'obbligo in capo agli Stati membri di istituire dei servizi di sostegno che siano in grado di affrontare le esigenze specifiche delle vittime del terrorismo, tra cui sostegno emotivo e psicologico per il trauma subito, consulenza ed informazioni su pertinenti questioni giuridiche o finanziarie, di modo da rispondere alle esigenze delle vittime e dei loro familiari immediatamente dopo un attentato terroristico e per tutto il tempo necessario.

Le necessità di adeguamento dell'ordinamento italiano sono risultate minime per conformare la normativa nazionale agli obblighi comunitari, limitati all'ampliamento dell'ambito di applicazione di fattispecie già esistenti.

Il 20 aprile 2016 la Commissione europea ha approvato la Comunicazione «Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per un'autentica ed efficace Unione della sicurezza», in cui si è posto l'accento sul pericolo rappresentato dai c.d. returnees, ovvero il rischio che i combattenti stranieri di ritorno in Europa possano fare uso di informazioni privilegiate per attività terroristiche, diffondere il verbo di Daesh[189] e radicalizzare altri individui, così da reclutarli.

[189] Organizzazione Stato Islamico (IS) o Daesh: dall'autunno del 2014, le autorità francesi fanno riferimento al gruppo terroristico come "Daesh". Il termine, a volte riportato come "Da'esh" o più raramente "Daiish". Si tratta dell'acronimo del nome arabo Dawlat al-Islamiyah f'al-Iraq wa al-

Il legislatore europeo chiede agli Stati membri di punire accanto all'istigazione diretta, anche tutte quelle condotte di c.d. "provocazione indiretta" suscettibili cioè di dare semplicemente luogo al rischio che possano essere commessi uno o più reati di questo tipo.

La direttiva (UE) 2016/1148, come abbiamo visto in precedenza, sulle misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS - Network and Information Security")[190], detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla Direttiva.

Negli anni si è andata diffondendo la consapevolezza che l'attuazione delle disposizioni contenute nella Direttiva da parte degli Stati membri non può avvenire se non attraverso una adeguata responsabilizzazione, a livello europeo, dei prestatori di servizi internet di hosting nella necessità assoluta di prevenire la diffusione in rete di contenuti terroristici per cui il 1º marzo 2018 la Commissione europea ha adottato una Raccomandazione sulle misure per contrastare i contenuti illegali on line 2018/334.

Le nuove misure mirano ad arrestare in maniera più efficace la pubblicazione e la diffusione di propaganda terroristica on line tra cui il processo di segnalazione, misure proattive per individuare tali contenuti, la rimozione efficace e introducono sistema di salvaguardia sufficienti per valutare accuratamente i contenuti terroristici.

Anche sul piano interno è stata creata una cornice di riferimento normativo. Intanto, è stato emanato il D.P.C.M. del 17 febbraio 2017, contenente indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, che ha ridisegnato l'architettura del nostro sistema di cybersecurity, al quale ha fatto seguito l'adozione, con D.P.C.M. del 31 marzo 2017, del Piano nazionale per la protezione cibernetica e la sicurezza informatica. Inoltre è importante segnalare il d.l. n.105 del 2019 convertito con l. 133 del 2019, del Perimetro di

---

Sham. Numerosi media in lingua araba fanno riferimento al gruppo in questo modo e molti arabisti concordano nel leggervi una sfumatura denigratoria, con la volontà della Francia di negare ai terroristi qualunque legittimazione.

[190] Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (GU n.132 del 9-6-2018).

sicurezza nazionale cibernetica che impone incisivi obblighi informativi a carico di tutte le amministrazioni pubbliche, enti e operatori pubblici e privati. Inoltre il c.d. decreto Cybersecurity ha determinato un ampliamento dei poteri speciali in materia di difesa e sicurezza nazionali attribuiti al Governo nell'ambito della disciplina dei c.d. Golden Power di cui al d.l. n.21/2012, convertito dalla l.n.56/2012.

Il decreto-legge n. 105 del 2019[191] mira a garantire un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.

In attuazione del decreto-legge n. 105 sono stati definiti in particolare il DPCM 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il DPCM 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC.

Infine, con il decreto-legge 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.

Prendendo atto della particolare gravità delle diffusioni in rete di contenuti di natura terroristica, le istituzioni europee hanno approvato il Regolamento 784/2021[192] (applicabile dal 7 giugno 2022) destinato a contrastare un uso improprio dei servizi di hosting per finalità terroristiche.

---

[191] Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ((e di disciplina dei poteri speciali nei settori di rilevanza strategica. Ha introdotto misure urgenti in materia di perimetro di sicurezza nazionale cibernetica e, sulla base di quanto disposto nel corso dell'esame del disegno di legge di conversione, disposizioni riguardanti la disciplina dei poteri speciali nei settori di rilevanza strategica.

[192] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici *online.*

Un insieme di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi di hosting[193], nel pieno rispetto dei diritti fondamentali. In particolare, il Regolamento, all'art. 3, prevede la facoltà per gli Stati membri di emettere a carico dei prestatori di servizi un ordine di rimozione di contenuti terroristici in tutti gli Stati membri.

Una volta ricevuto tale ordine, gli hosting providers dovranno provvedere alla rimozione del contenuto, prima possibile e, in ogni caso entro un'ora dal ricevimento dell'ordine stesso. I contenuti rimossi dovranno essere conservati dagli intermediari per almeno sei mesi per consentire le indagini del caso.

I prestatori di servizi di hosting devono adottare misure specifiche, efficaci e proporzionate (art. 5), basate su meccanismi automatici e automatizzati, garantendo verifiche specifiche, ove necessario, per tutelare i propri servizi dalla diffusione al pubblico di contenuti terroristici. Possono provvedere autonomamente alla rimozione dei contenuti pubblicati sulle proprie piattaforme ma il Regolamento sottolinea che coloro che forniscono i contenuti devono essere posti in grado di conoscere il motivo per cui tali contenuti siano stati rimossi o l'accesso disabilitato. Occorre anche predisporre un meccanismo di reclamo.

In caso invece di contenuti terroristici che comportino una minaccia imminente per la vita o un presunto reato di terrorismo, quale definito dalla direttiva 541/2017, i prestatori dovranno informare tempestivamente le autorità competenti.

Gli Stati membri designano le autorità competenti che dovranno poi coordinarsi e cooperare tra loro a livello sovranazionale.

Vengono fatte salve disposizioni contenute nella direttiva 31/2000, per cui rimane fermo il divieto di imporre un obbligo generale di ricerca attiva di contenuti terroristici a carico dei prestatori di servizi.

[193] In informatica si definisce servizio di hosting (dall'inglese to host, ospitare) l'allocazione delle pagine di un sito o di un'applicazione web su un server web. Ciò permette al sito o all'applicazione di essere raggiungibili e visibili agli utenti in rete. Tali servizi sono forniti dagli host o hosting provider.

Infine, per quanto riguarda le sanzioni gli Stati membri dovranno stabilire le norme relative al sistema sanzionatorio applicabile alle violazioni del Regolamento da parte dei prestatori di servizi di hosting, che potranno essere di natura amministrativa o penale.

La combinazione di un evento eccezionale (la pandemia) che ha funzionato da acceleratore e la moltiplicazione degli ambiti digitali hanno aumentato le superfici di attacco. Serve una nuova cultura e più collaborazione internazionale[194]

La sicurezza cibernetica oggi costituisce anche uno degli interventi previsti dal Piano nazionale di ripresa e resilenza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021 mentre il 14 aprile 2021 la Commissione Europea ha presentato la Strategia quinquennale contro la criminalità organizzata, indicando specifiche azioni per contrastarne, anche, la dimensione informatica[195].

I crimini informatici commessi da organizzazioni criminali sono, infatti, notevolmente accresciuti nel periodo di emergenza sanitaria da Covid 19 sia per numero che per livello di sofisticazione degli attacchi malware e delle frodi, in particolare, con riguardo ai mezzi di pagamento. Si stima che l'80 % dei reati della criminalità organizzata abbia natura digitale.

[194] IL SOLE 24 ORE, *Un salto di qualità per battere le cyberwar*, di Alessandro Curioni, 20/8/2021, p.11.

[195] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025-14 aprile 2021.

CAPITOLO TERZO

LA CYBERSECURITY IN TEMPO DI PANDEMIA

SOMMARIO: 3.1 Gli attacchi informatici più rilevanti della storia - 3.2 Cybercrime legati al Covid-19: dall'Agenzia europea per il farmaco ad Astrazeneca, dalla vicenda della Regione Lazio al caso Siae - 3.3 La sicurezza della rete: violato il sistema informatico dell'Europarlamento - 3.4 UE: il processo di digitalizzazione e il sostegno alla ripresa nel corso dell'emergenza sanitaria - 3.5 Strategie e modelli organizzativi per le imprese.

3.1 - Gli attacchi informatici più rilevanti della storia

Le più grandi potenze mondiali, come Cina, Stati Uniti d'America, Russia e Iran, effettuano investimenti colossali nella protezione delle proprie informazioni strategiche attraverso il potenziamento delle proprie difese informatiche. Questa tendenza è determinata dal fatto che, nel corso degli anni hanno dovuto pagare a caro prezzo la loro impreparazione davanti ad attacchi informatici che hanno segnato il corso della storia.

Tra gli attacchi più noti, rispettando una precisa cronologia, è da annoverare la "Guerra Fredda informatica" tra URSS e Stati Uniti.

La Guerra Fredda può definirsi come un evento storico caratterizzato da continue operazioni di spionaggio, anche a livello informatico. Un episodio significativo è quello avvenuto nel 1982, che ha visto gli americani prendere di mira i gasdotti russi. Gli Stati Uniti e la Russia combattevano per la supremazia politica. Fu una guerra di azioni non del tutto lecite, corse agli armamenti e inseguimenti tecnologici.

Il web, che all'epoca era agli albori della sua storia e veniva utilizzato per scopi militari, diventò terreno di conquista privilegiato per le due superpotenze. Dopo approfonditi studi la CIA[196] riuscì a trovare un modo per intrufolarsi nella rete del sistema

[196] Central Intelligence Agency, nota con la sigla CIA, è un'agenzia di spionaggio civile del governo federale degli Stati Uniti d'America, facente parte dell'United States Intelligence Community.

di controllo di un gasdotto siberiano utilizzando in una operazione militare i suoi tecnici al fine di violare il codice informatico russo. Riuscirono nel loro intento infettando la rete con una bomba logica, un sistema pronto a diffondere il suo codice malevolo al momento giusto.

I tecnici della CIA riuscirono a penetrare all'interno del sistema di gestione delle pompe del gas, che aveva il compito di verificare il funzionamento di un impianto ubicato in Siberia. Gli hacker statunitensi riuscirono a mandare in tilt il protocollo di sicurezza del sito, e provocarono l'aumento incontrollato della pressione all'interno del gasdotto. Di qui una potente esplosione e il propagarsi di un incendio di proporzioni terrificanti a testimonianza di come la guerra cibernetica avrebbe potuto sostituire un bombardamento di potenti ordigni.

Si capì subito la necessità di rafforzare i sistemi di sicurezza informatici. C'è chi ha parlato[197], invece, negli ultimi anni, proprio di una seconda guerra fredda originata dalla grande evoluzione che sta caratterizzando la Cina in ogni ambito e che vede anche gli USA concentrarsi contro i cinesi per ostacolare il loro allargamento sul territorio americano, come nel caso Google-Huawei[198].

Un malware risultato tra i più dannosi è stato sicuramente il Morris Worm. auto-replicante uno dei primi worm distribuiti attraverso Internet e il primo malware della storia a catturare l'attenzione dei media a livello mondiale.Vanta anche il primato di aver portato il suo creatore verso la prima condanna per pirateria informatica in America. Il codice del virus, da attribuire ad uno studente della Cornell University, Robert Tappan Morris[199], fu lanciato il 2 novembre 1988 dal laboratorio del MIT (Massachusetts Institute of Technology).

---

[197] F. RAMPINI, *La seconda guerra fredda*. Lo scontro per il nuovo dominio globale, Mondadori, 2019, p.ss .

[198] Nel 2019 Google toglie la licenza per Android a Huawei, a seguito dell'ordine esecutivo con cui Trump ha inserito Huawei in blacklist. Dopo l'elezione, la Casa Bianca accusa chiaramente Huawei e un'altra società cinese, Zte, di essere una minaccia per la sicurezza nazionale.

[199] Robert Tappan Morris (Massachusetts, 8novembre 1965), accademico, imprenditore e hacker di origine statunitense, docente al Massachusetts Institute of Technology.

«There may be a virus loose on the Internet». (Potrebbe esserci un virus libero di vagare nella rete). Questo l'allarme lanciato da Morris che lo ha reso famoso nel 1988. Del resto, il Morris worm nacque con lo scopo di valutare le dimensioni di Internet e non di arrecare danni, ma sfruttava alcune vulnerabilità di Unix sendmail, Finger, rsh / rexec e password.

Internet allora era costituita da poche decine di migliaia di computer interconnessi e quello che inizialmente doveva essere un progetto di ricerca si trasformó in una sorta di incubo. Morris fu la prima persona ad essere condannata per violazione del Computer Fraud and Abuse Act, una legge approvata solo due anni prima: tre anni di libertà condizionata, 400 ore di servizi socialmente utili e 10.050 dollari di multa. Oggi è docente al MIT Lab for Computer Science e qualche anno fa ha venduto a Yahoo!, al prezzo di 49 milioni di dollari, una start -up che lui stesso ha fondato, Viaweb Inc. Il termine Worm, invece, deriva dal romanzo di fantascienza del 1975 Codice 4GH (The Shockwave Rider)200 di John Brunner: i ricercatori che stavano scrivendo uno dei primi studi sul calcolo notarono delle similitudini tra il proprio programma e quello descritto nel libro per cui ne adottarono il nome.

Ha causato invece, danni per oltre 1 miliardo di dollari e si è diffuso nel 1999 prendendo a bersaglio i sistemi operativi Windows, attraverso i file Microsoft Word e il servizio di posta elettronica Outlook il pericoloso virus Melissa. Riusciva ad infettare i documenti con estensione .DOC e attraverso il client mail si auto-inviava ai primi 50 contatti presenti in rubrica, espandendosi così a dismisura.

Un giovane hacker, Jonathan James201 è l'autore di uno dei più famosi attacchi informatici della storia, dopo aver violato i sistemi di cyber security della più importante

---

200 J. BRUNNER, *The Shockwave Rider Harper Row*, Harper & Row, 1975. E' un romanzo di fantascienza di John Brunner. È noto per l'uso da parte del suo eroe delle abilità di hacking del computer per sfuggire all'inseguimento in un futuro distopico e per la coniazione della parola "worm" per descrivere un programma che si diffonde attraverso una rete di computer. Hacking o pirateria informatica stanno ad indicare l'intrusione in un sistema informatico da parte di hacker (pirati informatici) che riescono a sfruttare le lacune di sicurezza fino a quel momento ignorate. Sull'argomento: F. BARRESI, M. NIGRETTI, *Fenomeno Hacking. Analisi sociocriminalistica dell'intrusione informatica*, Iris4 Edizioni, Roma, 2012.

201 Jonathan Joseph James (1983 – 2008) è stato un hacker statunitense e il primo minorenne incarcerato per un crimine informatico negli Stati Uniti. Aveva 15 anni quando commise la sua

agenzia spaziale del mondo e della Defense Threat Reduction Agency (DTRA)[202], un'agenzia del Dipartimento della Difesa degli Stati Uniti che gli ha consentito di spiare documenti segreti attraverso la lettura di e-mail.

Nel 1999, il 30 giugno[203], il giovane riuscì ad infiltrarsi nei server della NASA, con un semplice Pentium. Ottenne l'accesso violando la password di un server dell'Agenzia Governativa dell'Alabama, libero di spostarsi all'interno della rete e di sottrarre molti documenti, ivi compreso il codice sorgente della Stazione Spaziale Internazionale.

La Shady RAT, invece, darà vita a una "pesca" molto pericolosa nelle profondità della rete. Rappresenta un sistema ben organizzato di cyber attacchi[204] di cui si dispongono dati certi solo dal 2006, anno in cui sono state verificate le avvenute compromissioni dei sistemi di sicurezza. È durato ben cinque anni, dal 2006 al 2011, anno in cui l'operazione illecita è stata individuata da Dmitri Alperovitch, membro del team di ricerca sulle minacce della società di sicurezza McAfee.

Si stima che l'operazione Shady RAT abbia colpito più di 70 grandi organizzazioni, comprese le Nazioni Uniti e altre istituzioni, attraverso uno spyware che infettava i dispositivi elettronici e, di conseguenza, ne estraeva i dati. Una email phishing comprendente un exploit veniva inviata ad un soggetto con un appropriato livello di accesso a sistemi informativi della compagnia. L'exploit, quando veniva aperto su un sistema non protetto, avviava il download di un malware che a sua volta apriva una comunicazione backdoor con il webserver Command & Control.

---

prima infrazione e 16 quando gli venne inflitta la sua prima condanna. Morì nella sua casa di Pinecrest, in Florida, il 18 maggio 2008 per una ferita d'arma da fuoco autoinflitta.

[202] DTRA è l'unica organizzazione del Dipartimento della Difesa focalizzata esclusivamente sulla lotta e sulla deterrenza delle armi di distruzione di massa e delle minacce emergenti. Collabora con il Dipartimento della Difesa, altri governi degli Stati Uniti e partner internazionali per preservare la pace offrendo capacità innovative, analisi obiettive, programmi efficaci e competenze di livello mondiale.

[203] J. OCONNELL, *10 Most Notorious Hackers of All Time*, hacked.com, 3 settembre 2015.

[204] A. CURIONI, *Il giorno del Bianconiglio,* Chiarelettere Editore, 2021, p. 1 ss.

Il malware esegue le istruzioni codificate attraverso commenti nascosti nel codice HTML di una pagina web che era stata intenzionalmente predisposta. Da quel momento i cybercriminali potevano accedere alla macchina infetta, scalare i privilegi utenti e stabilire nuovi punti di accesso con l'installazione del malware su altri sistemi. Iniziava così una vera e propria attività di spionaggio e la ricerca delle informazioni e dei dati che costituivano il fine dell'illecita intrusione nel sistema.

La Cina dispone di uno degli 'eserciti' più avanzati che opera nel cyber spionaggio. Si stimano 100.000 unità ed è considerata il nemico pubblico numero uno quando si parla di guerra cibernetica205. Verso la metà del 2009, pirati informatici esperti hanno scoperto almeno due criticità nel sistema di controllo dei server di Google fino a violarne l'accesso. L'attacco informatico denominato "Operazione Aurora", si è caratterizzato per l'accesso illecito alla banca dati di grosse aziende degli Stati Uniti, nei settori della sicurezza, difesa militare e ricerca tecnologica.

Secondo Google, l'offensiva sarebbe partita dalla Cina per cui la vicenda ha avuto inevitabilmente risvolti politici con una presa di posizione di figure istituzionali come il Segretario di Stato americano allora in carica, Hillary Clinton. Anche i programmatori del protocollo di sicurezza di Google furono colti impreparati non essendo a conoscenza dei punti deboli in cui si erano insinuati gli hacker. L'operazione Aurora ha cambiato il panorama dei rischi attacchi denial-of-service e il malware progettato per danneggiare o disabilitare le reti da attacchi mirati progettati per funzionare senza interruzioni e rubare informazioni inosservate. L'attacco informatico in questione è diventato la base di ciò che oggi è comunemente noto come Minaccia persistente avanzata (APT).

Un altro attacco informatico USA al nucleare iraniano divenuto famoso nel 2010 e da considerarsi tra i più pericolosi206 è il virus Stuxnet.

---

[205] C. S. GRAY, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling, Strategic Studies Institute*, Carlisle PA, April 2013, p.10 ss.

[206] Stuxnet è un virus informatico che si suppone sia stato creato e diffuso dal Governo americano nell'ambito dell'operazione "Giochi Olimpici", che consisteva in un'"ondata" di "attacchi digitali" contro l'Iran[in collaborazione col governo israeliano. anche se il fatto non ha mai trovato conferma.

Si tratta di una vera e propria offensiva messa in atto dal Governo americano e da quello israeliano contro la centrale nucleare iraniana di Natanz, attraverso un cyber virus che fu in grado di sabotarne il software di gestione delle centrifughe.

Il malware207 serviva a bloccare le turbine e, di conseguenza, tutta la produzione nucleare dell'impianto.

Tuttavia, i tecnici americani ne persero il controllo e il malware si propagò fuoriuscendo dalla centrale e insinuandosi in altri software acquistati da produttori esteri. Le loro aziende vennero infettate a loro volta e il problema divenne talmente vasto da far saltare la segretezza dell'operazione. Il blackout della struttura portò un ritardo nel programma di sviluppo nucleare del Paese. A causa della segretezza del programma iraniano, non ci sono dati confermati sulla portata del danno subito. Ma è da ritenere che il programma di arricchimento dell'uranio abbia subito un rallentamento importante dopo aver messo fuori uso almeno 1.000 delle 5.000 centrifughe iraniane.

Nel 2012, invece, le due multinazionali Visa e Mastercard in ambito bancario sono state oggetto di attacchi che hanno comportato il furto dei dati di circa 10 milioni di carte di credito. Mastercard è stata particolarmente colpita poiché in passato, nel 2005, era già stata bersagliata nei suoi meccanismi di difesa cibernetica avendo subito il furto delle credenziali di milioni di clienti. Nel 2018, altre banche, tra cui Bnl, Gruppo Carige, Fineco Bank e Intesa Sanpaolo, erano finite nel mirino degli hacker che sfruttando il malware Danabot, erano state capaci di manipolare e accedere a dati di portali di home banking e di posta elettronica.

Il malware Zeus/Panda rubava password, token e cookie a istituti bancari o finanziari colpendo Credem, Fineco, Gruppo Carige, Intesa Sanpaolo, Poste, Quercia, Banca Passadore, Friuladria, Bper e Inbank. Nel 2019 ad Unicredit sono stati violati dati per milioni di utenti e l'istituto di credito già nel 2017 era stato oggetto di un doppio attacco con la violazione di dati dei clienti con prestiti attivi presso la Banca. All'inizio del periodo di lockdown, nel 2020, un attacco informatico ha permesso a un gruppo di hacker l'accesso a caselle di posta elettronica di alcuni dipendenti della Mps con messaggi fraudolenti di

[207] N.P. ROMASHKINA, A. V. ZAGORSKI, *Information security threats during crises and conflicts of the XXI century* 2016, Moscow, p.15.

posta vocale allegati e inviati a numerosi clienti della banca senese. In sostanza gli hacker entravano nelle email aziendali e i correntisti del Monte Paschi di Siena ricevevano false mail dalla banca.

Una spia può nascondersi anche nelle camere d'albergo generando quello che viene definito il Darkhotel. Questo tipo di attacco ha colpito i clienti degli hotel a partire dal 2012 con conseguenze pesanti per top manager e personalità di spicco.

L'attacco si fa largo nei computer delle vittime principalmente attraverso la rete Wi-Fi degli hotel. I cybercrimiali hanno utilizzato degli exploit zero-day presenti in Adobe Flash e altri prodotti popolari appartenenti a noti fornitori.

Quando si collegavano alla rete dell'hotel, gli veniva richiesto di installare un aggiornamento che apparentemente sembrava legittimo anche perché il software risultava piuttosto diffuso e popolare. I dispositivi venivano infettati dallo spyware DarkHotel, introdotto volutamente nella rete dai cybercriminali qualche giorno prima dell'arrivo di personalità per poi essere rimosso a distanza di qualche giorno. Lo spyware, in sostanza, registrava in segreto i tasti digitati dalla vittima e ciò consentiva di organizzare attacchi phishing mirati. Il malware usato nella campagna Darkhotel (conosciuta anche come Tapaoux), tuttavia era apparso per la prima volta già nel 2007 e i ricercatori di sicurezza hanno scoperto connessioni risalenti al 1 gennaio del 2009. Hotel e catene, anche negli anni successivi, hanno denunciato a più riprese questi attacchi noti come 'invisibili' perché impossibile da verificare in loco se non dagli estratti conto degli ospiti208.

L'aeroporto di Fiumicino ha registrato una giornata nera per la sicurezza informatica

il 1° aprile del 2015 quando le telecamere subirono un attacco a livello informatico. Un responsabile della sicurezza si accorse che oltre 100 telecamere erano malfunzionanti e inviò una segnalazione interna con cui si metteva in guardia circa un grave problema con le telecamere di Hikvision che tentavano di registrarsi presso un server esterno, un indirizzo IP ancora oggi sconosciuto. In un'ora furono registrati 11mila tentativi di connessione forse nel tentativo di trasferire dati o di consentire a qualcuno di controllare il sistema di videosorveglianza in un luogo strategico per l'Italia.

[208] IL MESSAGGERO, *Hacker, la minaccia ci aspetta in albergo*, di Francesco Malfetano, 8 luglio 2019, p.15

Il dato allarmante oggetto anche di una recente inchiesta del programma televisivo Report è che le telecamere di Hikvision sono presenti in numerosi palazzi istituzionali italiani: Ministeri, tribunali, palazzi dei servizi di sicurezza e addirittura Palazzo Chigi.

Il controllo di Hikvision è nelle mani di CETC, un'azienda dello Stato cinese che sviluppa software militari, infrastrutture di difesa, armi elettroniche,, per il 46%, nelle mani di un gigante legato allo stato militare cinese.

Un attacco globale a Internet si è verificato attraverso il malware, Mirai, in grado di infettare i dispositivi della "Internet of Things" (IoT) (videocamere di sorveglianza, videoregistratori digitali e altri device connessi a Internet) e utilizzarli per portare attacchi coordinati.

Ha fatto la sua comparsa nel 2016[209] con una serie di attacchi che sono andati via via crescendo, tra cui quello che ha bloccato parte degli Stati Uniti per diverse ore.

Si è trattato di un attacco DDoS[210]. Gli attacchi Distributed Denial of Service (DDoS) impiegano delle botnet (reti di computer o dispositivi connessi a Internet sotto il controllo di pirati informatici) con cui colpiscono siti Web e infrastrutture informatiche provocandone il blocco.

Almeno due imponenti attacchi di Distributed Denial of Service (abbreviato in DDoS) hanno messo in ginocchio DynDNS, l'importante infrastruttura online che abbina nomi di dominio a indirizzi IP di importanti destinazioni, come Twitter, Amazon, Tumblr, Skype, Reddit, The New York Times, PayPal, Spotify e Netflix.

Le linee della società si saturano e diventano inaccessibili così subentra un malware utilizzato per mettere fuori gioco la compagnia Dyn.

Dyn non è riuscita a contrastare l'attacco DDoS così potente; il DNS e altri servizi che vi si appoggiavano non erano più disponibili, e ciò ha avuto conseguenze importanti su

[209] T.G. PALLA, S. TAYEB, *Intelligent Mirai Malware Detection for IoT Nodes*. Electronics, 2021, Academic Editor: Taeshik Shon, 24 May 2021, p.1.

[210] CORRIERE DELLA SERA, *Gli hacker nel frigorifero*, di Federico Cella, 23 ottobre 2016, p.10.

piattaforme online molto popolari e altri servizi statunitensi. Dyn alla fine è riuscita a recuperare ma l'escalation di Mirai[211] lascia riflettere sulla sicurezza dei dispositivi.

NotPetya/ExPetr è stato, invece, l'attacco informatico più costoso. Si tratta di un wiper il cui nome è ExPetr o anche Nepeta che ha colpito principalmente l'Europa negli anni 2016 e 2017 . Il principio di base era lo stesso di WannaCry: sfruttando gli exploit EternalBlue ed EternalRomance, il worm aveva la capacità di muoversi nel Web, cifrando qualsiasi dato trovasse lungo il suo passaggio.

Nonostante il numero di dispositivi infettati sia stato inferiore, l'epidemia NotPetya[212] ha colpito soprattutto le aziende. I cybercriminali sono riusciti a prendere il controllo del server di aggiornamento di MeDoc per cui molti clienti che utilizzavano questo stesso software hanno preso il malware che assumeva le sembianze di un aggiornamento e si diffondeva indisturbato attraverso la rete. Si calcola che l'attacco informatico NotPetya abbia provocato danni pari a 10 miliardi di dollari, mentre WannaCry ha raggiunto un range di 4-8 miliardi di dollari. Fino ad oggi, siamo di fronte all'attacco informatico che è riuscito a provocare più danni economici in assoluto.

Con WannaCry, l'attacco ransomware venne lanciato in tutto il mondo. Un trojan molto particolare che si è diffuso nel maggio del 2017 sfruttando un punto vulnerabile di Windows capace di infettare centinaia di migliaia di computer distribuiti, si calcola, in almeno 150 Paesi diversi.

Si calcolano oltre 230.000 computer raggiunti, uno dei maggiori contagi informatici mai avvenuti. Si è scoperto che WannaCry riesce a sfruttare una vulnerabilità di SMB tramite un exploit chiamato EternalBlue, che si ritiene sviluppato dalla National Security Agency statunitense per attaccare sistemi informatici basati sul sistema operativo Microsoft Windows. EternalBlue era stato sottratto da un gruppo di hacker che si fa chiamare The Shadow Brokers e pubblicato in rete il 14 aprile 2017.

---

[211] LA STAMPA, *Chi sono i pirati della cyberguerra*, di Gianni Riotta, 23 ottobre 2016, p.19.

[212] LA REPUBBLICA, *Petya, l'ultimo attacco hacker mondiale*, di Rosalba Castelletti, 28 giungo 2017, p.15.

Il malware viene diffuso per mezzo di finti account email e, dopo che viene installato su un computer, comincia a infettare altri sistemi presenti sulla stessa rete e quelli vulnerabili esposti a internet, che vengono infettati senza alcun intervento dell'utente.

Quando infetta un computer, WannaCry cripta i file bloccandone l'accesso e aggiunge l'estensioneWCRY; impedisce inoltre il riavvio del sistema. A quel punto, in un file denominato Please_Read_Me@ si trova una richiesta di riscatto che l'utente deve pagare in bitcoin[213] per avere lo sblocco dei file.

WannaCry, chiamato anche WanaCrypt0r 2.0, è un worm, di tipologia ransomware, responsabile di un'epidemia su larga scala su computer con Microsoft Windows. In esecuzione cripta i file che si trovano sul pc e avanza una richiesta di riscatto di alcune centinaia di dollari per decriptarli.

Il 12 maggio 2017 il malware è riuscito ad infettare i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo, tra cui Portugal Telecom, Deutsche Bahn, FedEx, Renault, il National Health Service, il Ministero dell'interno russo nonchè l'Università di Milano-Bicocca. Ha colpito quindi infrastrutture critiche: in alcuni ospedali, WannaCry ha cifrato tutti i dispositivi, apparecchiature medicali comprese e alcune aziende sono state costrette a bloccare il ciclo produttivo. L'Europol ha avviato una indagine per scoprire i responsabili dell'attacco e per monitorare la situazione.

La particolarità di WannaCry sta nel fatto che per permettere l'accesso di un trojan, l'utente deve compiere una specifica attività come ad esempio cliccare su un link suggerito. WannaCry invece, non avendone necessità non richiedeva questo passaggio e si propagava

[213] Il bitcoin è una moneta elettronica da usare tramite Internet, attraverso una rete di codici sicura, impossibile da manipolare da parte di terzi. Si tratta di una valuta libera e decentralizzata, a disposizione di chiunque e ovunque riesca ad arrivare una connessione Internet. Le criptovalute, come confermano anche gli esperti di Bitcoin Prime, sono caratterizzate da un livello altissimo di privacy. I Bitcoin si basano sulla tecnologia blockchain. Per poterli scambiare è necessario un software (detto wallet) che assegna un numero ID (identificativo) col quale si viene univocamente riconosciuti su questo canale e che viene gestito tramite una chiave privata (password). Il codice ID è alfanumerico e non permette di risalire all'identità dell'attore.

in maniera inarrestabile. L'Amministrazione Trump accusò la corea del Nord di avere organizzato il cyber attacco[214].

L'attacco è stato fortemente rallentato, quando si arrivò, grazie alla giusta intuizione di un giovane ricercatore britannico di soli 22 anni, Marcus Hutchins[215], alla soluzione per contrastarlo scoprendo che bastava registrare un dominio.

Infatti, il giovane riuscì a scoprire che prima di infettare un computer WannaCry cerca di contattare un indirizzo web, che in quel momento non risultava registrato.

Dopo aver registrato il dominio, è stata notata una rapida diminuzione delle infezioni del worm.

Fino a quel momento, i responsabili avevano chiesto dai 300 ai 600 dollari di riscatto per decriptare e restituire i dati trafugati all'interessato. Il ransomware si è diffuso a macchia d'olio ed ha portato al blocco di grandi Aziende di dimensioni internazionali[216].

Anche il gigante Facebook è finito, negli ultimi anni, più volte, sotto attacco hacker. A causa di queste violazioni nel 2021 si è scoperto[217] che i dati privati di 533 milioni di utenti, registrati in 106 Paesi nel mondo, sono disponibili in rete. Di questi, 35 milioni sono italiani, circa il 90% delle persone che nel nostro Paese utilizza il social network, 32 milioni sono negli Stati Uniti, 11 milioni nel Regno Unito, circa 6 milioni in India, etc.

I dati rubati sono essenzialmente numeri di telefono e in alcuni casi nomi, cognomi, date di nascita oppure indirizzo di posta elettronica, compresi addirittura i dati personali di

[214] LA REPUBBLICA, *Attacco Wannacry così Trump accusa Pyongyang* di Federico Rampini, 20 dicembre 2017, p.18.

[215] Marcus Hutchins (nato nel 1994), noto anche online come MalwareTech , è un ricercatore britannico di sicurezza informatica noto per aver bloccato temporaneamente l' attacco ransomware WannaCry . È impiegato dalla società di sicurezza informatica Kryptos Logic. Hutchins è di Ilfracombe nella contea del Devon .

[216] C. FREDIANI, *Cybercrime. Attacchi globali, conseguenze locali*, Hoepli, 2019.

[217] TGCOM24, 06 aprile 2021, 12:13.

Zuckerberg. Il database con i dati rubati è stato reso disponibile gratuitamente per tutti. A confermare il fatto, un rapporto pubblicato da Business Insider[218].

In realtà si tratterebbe dello stesso gruppo di dati sottratti al social network nel 2019, tanto che la portavoce di Facebook, Lily Sheperd, ha affermato che i dati «sono vecchi e il furto era stato già segnalato nel 2019 e il problema risolto nell'agosto di quell'anno».

Il timore è che i dati rubati ad oltre mezzo miliardo di profili anche se vecchi di alcuni anni potrebbero essere utilizzati per sottrarre identità e commettere frodi online sfruttati dai criminali facilmente accessibili e facili da utilizzare. Facebook, ormai da anni, è alle prese con problemi riguardanti la sicurezza dei dati.

Il caso più clamoroso e controverso è stato, senza dubbio, quello legato allo scandalo del 2018, quando fu rivelato che la società Cambridge Analytica[219] aveva avuto accesso alle informazioni di 87 milioni di utenti Facebook e li aveva utilizzati per scopi di propaganda politica[220]. Un momento di spartiacque nella comprensione pubblica del valore dei dati personali che ha provocato un significativo calo del prezzo delle azioni di Facebook.

In realtà la raccolta illecita di dati personali da parte di Cambridge Analytica[221] era stata segnalata per la prima volta nel dicembre 2015 da Harry Davies, giornalista di The Guardian che riferiva che Cambridge Analytica stava lavorando per il senatore degli Stati Uniti Ted Cruz utilizzando i dati raccolti da milioni di account Facebook senza il consenso degli interessati.

---

[218] *Business Insider* è un sito web d'informazione statunitense creato a New York, nel 2007 da Kevin Ryan.

[219] La Cambridge Analytica (CA), una società di consulenza britannica il cui nome è divenuto celebre a seguito dello scandalo per la gestione dei dati per influenzare le campagne elettorali. Il 2 maggio 2018 la società ha dichiarato la bancarotta a causa dello scandalo in cui era stata travolta con Facebook per aver contribuito alla manipolazione del pensiero degli elettori con una propaganda elettorale segreta a favore di Trump alle presidenziali americane del 2016 ed al referendum inglese pro Brexit.

[220] N.TIRINO, *Cambridge Analytica. Il potere segreto, la gestione del consenso e la fine della propaganda*, Lecce, Libellula Edizioni, 2019, p.51 ss.

[221] C.WYLIE, *Il mercato del consenso: come ho creato e poi distrutto Cambridge Analytica*, Milano, Longanesi, 2020.

Ulteriori informazioni sono state aggiunte in ulteriori pubblicazioni ma Facebook si era rifiutata di commentare gli articoli pubblicati.

Lo scandalo scoppiò solo a marzo 2018 a causa delle rivelazioni di un whistleblower, un ex dipendente della Cambridge Analytica, divenuto una fonte anonima per un articolo nel 2017 per The Observer[222] dal titolo "The Great British Brexit Robbery". L'articolo divenne virale ma non fu ritenuto credibile da molti e ripreso da altre testate il 17 marzo 2018 causando grande clamore e sconvolgendo l'opinione pubblica[223].

Oltre 100 miliardi di dollari vennero così eliminati dalla capitalizzazione di Facebook.

Lo scandalo, alla fine, ha portato Facebook Mark Zuckerberg ad accettare di testimoniare davanti al Congresso degli Stati Uniti e patteggiò una somma record di 5 miliardi di dollari con la Federal Trade Commission per chiudere la questione legata alle violazioni della privacy.

L'evento fu molto significativo e di forte impatto tanto che accese inevitabilmente i riflettori sugli standard etici dei social media, delle organizzazioni per la consulenza politica, e degli stessi politici[224].

[222] The Observer è un periodico britannico della domenica, edito dallo stesso gruppo del Guardian e dell'internazionale Guardian Weekly, il più antico giornale domenicale del mondo. Il suo primo numero risale al 4 dicembre 1791.

[223] https://www.corriere.it/sette/esteri/19_novembre_15/ex-ragazza-cambridge-analytica-manipolavamo-tutto-voti-comportamenti-coscienze-b754fc80-055d-11ea-a1df-d75c93ec44da.shtml

[224] *CORRIERE DELLA SERA, Hacker mobilitati per le elezioni USA,* di Massimo Gaggi, 5 luglio 2019, p.27.

3.2 Cybercrime legati al Covid-19: dall'Agenzia europea per il farmaco ad Astrazeneca, dalla vicenda della Regione Lazio al caso Siae.

È facile immaginare come un evento di carattere così eccezionale come la pandemia, con tutto il suo carico emotivo, con un flusso continuo di nuove informazioni (con i cambiamenti delle modalità di lavoro e delle abitudini di vita) e di provvedimenti normativi, possa aver creato un terreno particolarmente fertile per gli autori di campagne di phishing e non solo. Da inizio 2020[225]le società che operano nella cybersecurity in Borsa hanno guadagnato il doppio. Infatti l'indice ISE Cyber Security è salito del 60% contro il 30% dell'Msci World (indice di mercato azionario costituito da migliaia di titoli di livello globale)

Soprattutto nel primo periodo almeno il 10% delle nostre mailbox conteneva mail a tema COVID-19. Oltre a mail di spam vere e proprie, relative a prodotti e servizi (mascherine, gel, termoscanner, guanti, test antigenici, tamponi, servizi finanziari, etc.) questo flusso diffondeva anche mail di phishing e distribuzione di malware che sfruttavano l'alto livello di attenzione legato alla particolare situazione che si stava vivendo.

Tra le tecniche più usate, le campagne messe in atto con finte mail che annunciavano ai malcapitati la perdita del posto di lavoro. La mail, che sembrava provenisse dal dipartimento risorse umane, comunicava al malcapitato il suo licenziamento in tronco per giustificato motivo: ossia l'emergenza sanitaria da Covid 19 in corso.

Si capisce, dunque, perché l'email security al tempo della pandemia[226] abbia assunto un ruolo di primo piano e come siano cambiate sia le modalità di comunicazione sia le tecniche offensive adottate dai cyber criminali.

Sfruttando l'elemento emozionale del momento, gli attacchi hanno riguardato anche finalità di spionaggio industriale o di information warfare.

---

[225] IL SOLE 24 ORE, *La cybersecurity tra gli affari di Borsa*, 6 agosto 2021, p.25.

[226] A. MUKHOPADHYAY, A. PRAJWAL, *A robust framework for prevention of cyber attacks in the Covid era*, 2a Conferenza Internazionale per le Tecnologie Emergenti, INCET 2021.

Fortunatamente, questi attacchi non hanno provocato danni estremamente gravi pur avendo colpito target importanti quali università, enti governativi, forze dell'ordine e, non da ultimo, il settore sanitario.

Sono aumentate le criticità di alcune strutture statali e gruppi black-hacker in tutto il mondo che hanno sfruttato la fase emergenziale facendo emergere i punti di maggiore criticità per uno Stato.

Sono arrivati così attacchi a molti Paesi dell'Unione, molto spesso perpetrati ai danni delle strutture sanitarie pubbliche.

È evidente che sostenere che l'Italia e l'Europa si trovano sotto attacco informatico e politico non può considerarsi corretto. Altra cosa è preoccuparsi del fatto che esiste il rischio che gruppi esteri stiano prendendo di mira il nostro sistema sanitario incredibilmente fragile.

Le restrizioni introdotte con il lockdown, hanno senz'altro intensificato l'utilizzo della rete Internet per l'esecuzione di transazioni commerciali, comportando un correlato incremento dei reati informatici, specie il furto di identità.

In Portogallo[227], nel frattempo, si è avuta una rapida diffusione del reato di frode informatica, grazie alla possibilità di effettuare acquisti telematici associando il proprio numero telefonico al conto bancario, il cosiddetto MB-WAY. Migliaia gli accessi non autorizzati sui conti correnti di utenti che hanno fornito i propri dati personali, confidando nella possibilità di effettuare come sempre normali acquisti in rete. I responsabili sono stati individuati: si tratta di un'associazione criminale di origine moldava. Anche nel Regno Unito la minaccia della criminalità informatica si è intensificata, sia come numero che come gravità di casi e così la percentuale di e-mail di phishing rilevate e connesse alla tematica del Covid-19 è aumentata in tutta Europa.

Il numero di cyber crimes si è impennato rispetto al periodo pre-lockdown come vedremo meglio nel capitolo successivo. Altrettanto dicasi per i reati di pedopornografia on line, accentuati dal crescente numero di ore giornaliere trascorso dai minori sul web dopo la chiusura delle attività scolastiche.

[227] REPORT 3/2020, Organismo permanente di monitoraggio ed analisi sul rischio di infiltrazione nell'economia da parte della criminalità organizzata di tipo mafioso, Ministero dell'Interno, Roma, luglio 2020, p.22.

Nella prima fase del Covid-19 si segnalava l'utilizzo della rete per diffondere false informazioni sulla pandemia, parallelamente all'esecuzione di veri e propri attacchi cibernetici a siti istituzionali di diversi Paesi.

Ora sembra acquisita e diffusa la consapevolezza dei rischi connessi alla diffusione del Covid-19 mentre vengono ancora registrati cyberattacchi ai siti di enti e istituzioni coinvolte nella cura e nell'assistenza alla popolazione.

I principali obiettivi sono stati i siti web di diverse istituzioni pubbliche, sia in Romania che in Moldavia[228]. Il gruppo criminale operava attacchi informatici "ransomware", nel periodo immediatamente successivo alla crisi sanitaria, ai danni di istituzioni di sanità pubblica, generalmente ospedali, utilizzando un'applicazione dannosa mascherata in una e-mail sotto forma di un file che apparentemente risultava provenire da altre istituzioni governative, riguardante consigli sulla minaccia Covid-19.

Un'attività congiunta tra autorità giudiziaria speciale rumena e moldava ha consentito di individuare e disarticolare un gruppo criminale organizzato, denominato "Pentaguard", specializzato nella commissione di reati informatici.

Hanno fatto notizia, inoltre, numerosi data breach, come nel caso che ha visto protagonista la società Campari[229], a cui sono stati trafugati due terabyte di dati con la minaccia di renderli pubblici se non fosse stato pagato un riscatto. L'attacco è stato subito notificato alle autorità competenti per la protezione dei dati, alla Polizia Postale italiana e all'FBI. Nemmeno i colossi del web sono stati risparmiati dalla perdita di dati e da episodi criminali: oltre a Facebook, le violazioni hanno riguardato anche utenti di TikTok, Instagram e YouTube.

In un periodo segnato dalla pandemia, non sorprende che molti tentativi di furto di dati e informazioni abbiano riguardato l'ambito sanitario: basti pensare all'Agenzia Europea del Farmaco (EMA)[230] che ha subito un cyber attacco in cui sono stati violati documenti sul vaccino Pfizer, mentre un gruppo di hacker nordcoreani ha effettuato

[228] REPORT 3/2020, Organismo permanente di monitoraggio ed analisi sul rischio di infiltrazione nell'economia da parte della criminalità organizzata di tipo mafioso, Ministero dell'Interno, Roma, luglio 2020, p.22.

[229] https://www.cybersecurity360.it/nuove-minacce/ransomware/campari-furto-dati-con-minaccia-perche-ce-boom-di-questi-attacchi-e-come-difendersi/

[230] ANSA, *Cyber-attacco all'Ema, obiettivo il vaccino Pfizer*, Roma, 10 dicembre 2020.

tentativi di intrusione nei sistemi della casa farmaceutica AstraZeneca[231] nelle varie fasi di sperimentazione che hanno preceduto l'uscita sul mercato del vaccino.

Tra i problemi di sicurezza rilevati nel pieno della pandemia spiccano quelli che hanno coinvolto le applicazioni di video-conferenza e meeting virtuali approfittando del ricorso allo smart working[232] in un contesto globale in cui il ricorso al lavoro flessibile era ancora limitato ed è stato reso possibile dalla diffusione di tecnologie digitali.

Il caso più celebre è da ritenersi quello che ha colpito la piattaforma Zoom[233], il fenomeno dello "zoombombing", per cui utenti non registrati potevano irrompere in chat di riunioni non solo per condividere con gli altri utenti contenuti inappropriati, ma anche per trafugare dati sensibili e registrazioni che sono stati poi pubblicati online.

A luglio 2021 è stata la volta della regione Lazio. Un attacco informatico al data center che ospita i sistemi informatici ha compromesso l'utilizzo di alcuni dei servizi e delle applicazioni a disposizione del cittadino.

Il sistema informativo regionale si è subito attivato per evitare ulteriori conseguenze sulla privacy dei cittadini e la sicurezza dei dati personali in possesso dell'Ente Regione. Una organizzazione criminale transnazionale ha attaccato i dati sensibili di una gran fetta della popolazione vaccinale fino a rendere impossibile le prenotazioni[234].

È stato tempestivamente attivato, in collaborazione con le autorità competenti e le forze dell'ordine, un team tecnico dedicato alla gestione dell'evento e sono state messe in campo le misure necessarie per rimediare a possibili violazioni dei dati personali. Le misure adottate hanno comportato la sospensione di alcuni servizi importanti anche a distanza di

---

[231] LA STAMPA, *Covid, sette attacchi hacker ai server di AstraZeneca di E. Izzo,* 30 dicembre 2020.

[232] F. DI MASCIO, S. ANGELETTI, A. NATALINI, *Lo smart working nelle pubbliche amministrazioni centrali ai tempi del COVID – 19,* Rivista Italiana di Politiche Pubbliche, Il Mulino, 1/2021, aprile.

[233] Zoom Video Communications è una società di servizi di teleconferenza con sede a San Jose in California; fornisce servizi di conferenza remota che combina videoconferenza, riunioni online, chat e collaborazione mobile. Parallelamente alla grande diffusione della piattaforma Zoom, però, è stato segnalato il cosiddetto "Zoombombing", cioè la pratica di interrompere videolezioni e riunioni di vario genere in corso con messaggi offensivi o, nei casi peggiori, pornografici o razzisti.

[234] LA REPUBBLICA, 2 agosto 2021, *Attacco hacker ai dati del Lazio. Stop ai vaccini, chiesto un riscatto,* di Arianna Di Cori e Romina Marceca, p.10

alcuni mesi. I disagi ai sistemi informatici sono continuati ed hanno rallentato i servizi essenziali, tra cui tamponi e green pass.

I problemi hanno riguardato diversi settori collegati al servizio sanitario regionale, dalle farmacie alle forniture ospedaliere, ma anche il mondo delle professioni e del lavoro.

Criticità sono emerse nei pagamenti di fatture emesse a ridosso dell'attacco informatico, e nelle compravendite immobiliari a causa del portale dedicato alle attestazioni energetiche.

Sul sito web della Regione Lazio su più pagine, contrassegnate da un asterisco, un messaggio avvertiva l'utenza che a causa di un attacco hacker alcuni servizi non erano raggiungibili. Dopo trenta giorni il bilancio predisposto dalla Regione Lazio vedeva attivi 23 servizi su 36 totali.

Anche i Pm dell'antiterrorismo indagano sull'attacco hacker alla Regione Lazio.

I reati contestati vanno dall'accesso abusivo a sistema informatico alla tentata estorsione fino all'aggravante delle finalità di terrorismo[235]. Tra le fattispecie di reato ipotizzate dai pm, risulta anche il danneggiamento al sistema informatico. In base a quanto accertato, l'attacco sarebbe partito dall'estero con rimbalzo in Germania, anche se non conosciuta la matrice di provenienza.

Purtroppo non si tratta di un caso isolato. Nel marzo del 2020 gli hacker avevano preso di mira il San Raffaele di Milano e ad aprile dello stesso anno l'ospedale Spallanzani di Roma. Senza contare gli attacchi non resi pubblici. L'intelligence ha da tempo allertato la rete sanitaria nazionale invitandola ad innalzare le difese su reti ed infrastrutture ponendo intelligentemente una barriera di protezione

Un altro episodio si è verificato alla Asl Roma 3[236], che comprende tutto il territorio di Ostia, un bacino d'utenza molto ampio nella capitale. Qui potenzialmente erano a rischio i dati di circa 600mila cittadini.

---

[235] CORRIERE DELLA SERA, *Hacker, dati e stipendi a rischio. Ora i pm indagano per terrorismo,* di Rinaldo Frignani, 4 agosto 2021, p.2.

[236] QUOTIDIANO SANITÀ, *Roma. Attacco hacker all'ospedale San Giovanni. Ma nessun blocco delle attività cliniche,* 13 settembre 2021, http://www.quotidianosanita.it/regioni-e-asl/articolo.php?articolo_id=98174

In ultimo anche l'attacco informatico, dopo il grande black-out del CED della Regione Lazio, all'ospedale San Giovanni di Roma. Un allarme preoccupante per il sistema sanitario regionale. Un attacco hacker con virus ransomware che ha paralizzato l'attività informatica della struttura sanitaria, una delle più grandi della capitale, e messo a rischio migliaia di visite e interventi prenotati o da prenotare a meno di due mesi dal blitz che ha messo in ginocchio la regione Lazio[237].

Ad agosto lo stesso virus ha 'bucato' il sistema di sicurezza informatico dell'Agenzia regionale di sanità Toscana con la stessa tipologia di malware del Lazio colpendo file epidemiologici[238].

Lo scorso anno la Procura di Roma ha formalmente aperto un fascicolo di indagine per tentata estorsione e accesso abusivo a sistema informatico anche in seguito all'attacco hacker subito dalla Siae. Delle indagini si occupa la polizia postale. Dalle prime verifiche alcuni dati, pare solo dati anagrafici e carte di identità di alcuni artisti, sarebbero comparsi sul dark web. Alcuni personaggi famosi, tra cui Al Bano e Samuele Bersani, sono stati vittime proprio di azioni estorsive da parte di hacker.

Gli hacker del gruppo Everest hanno posto in vendita i dati sottratti alla Siae per 500.000 dollari. Lo fanno sapere loro stessi attraverso un sito ufficiale sottolineando come la società Siae non abbia voluto scendere a patti.

E poi, un messaggio rivolto agli stessi artisti: «Rappresentanti delle celebrità, contattatemi per riscattare i dati. Dopo la vendita i dati saranno cancellati».

Una parte dei documenti è disponibile gratuitamente: dalla pagina del gruppo Everest è infatti possibile ricevere un link, con relativa password, per scaricare 1.58 gb di documenti, che loro sostengono si tratti solo di una minima parte dei dati rubati. Ci sono 5200 file relativi a dati anagrafici, indirizzi mail e numeri di telefoni, ma anche iban bancari, oggetto dell'accesso fraudolento al sistema Siae.

La società sarebbe intervenuta subito, mettendo in atto misure rafforzative di sicurezza con il coinvolgimento di società di Cyber Security di assoluto livello e di

---

[237] CORRIERE DELLA SERA, *Gli hacker attaccano l'ospedale, caos al pronto soccorso,* di Rinaldo Frignani, 14 settembre 2021, p.19.

[238] LA REPUBBLICA, *Dopo il riscatto alla Regione Lazio, hacker violano un server della sanità Toscana,* 20 agosto 2021, p.16

indiscussa capacità nella gestione degli incidenti di sicurezza, delle attività di recovery e protezione, in grado di affiancare Siae nel fronteggiare la particolare capacità criminale degli aggressori, già noti alle forze dell'ordine».

Una denuncia è stata presentata alla polizia postale insieme a una notifica di violazione al Garante per la protezione dei dati personali. Dopo l'attacco sferrato con la sottrazione di oltre 60 gigabyte, è stato chiesto un riscatto di 3 milioni di bitcoin. A supportare gli investigatori italiani nelle indagini c'è anche Europol. L'attacco avrebbe avuto origine da un Ip russo.

In ultima analisi il blackout globale che intorno alle 17,40 del 4 ottobre scorso, ha reso inaccessibili al mondo Facebook, Instagram e WhatsApp e solo verso l'una di notte (ora italiana) hanno ripreso gradualmente a funzionare. Solo in seguito sono pervenute le scuse di Mark Zuckerberg[239] per il gigantesco blackout globale: «Scusate per l'interruzione, sappiamo quante persone fanno affidamento sui nostri servizi per restare connesse».

Non esiste alcuna conferma su ciò che effettivamente abbia causato l'incidente ma è possibile che il problema risieda nel protocollo BGP o DNS, obiettivi popolari tra i criminali informatici.

Si possono avere vari potenziali attacchi contro l'infrastruttura DNS, dagli attacchi DDoS al rebinding DNS locale o all'hijacking di un DNS con il social engineering contro il registrar, sicuramente meno popolari dei comuni attacchi malware e ransomware, ma estremamente devastanti se riescono ad avere successo in un attacco sofisticato.

Sembrava di assistere all'inizio di un romanzo distopico in cui viene presagita un'esperienza di vita sconvolgente sulla fine del mondo digitale. Alle 17.30, ora italiana, il sistema di piattaforme di Menlo Park ha cominciato a dare segni di cedimento e poi il black out. I social oscurati in ogni parte del mondo. Il blocco è durato oltre sette ore, l'interruzione di servizio più lunga dal 13 marzo del 2019. Un fermo che secondo la piattaforma Netblocks[240] ha causato un danno all'economia mondiale di 1.129.959.864 dollari.

---

[239] Mark Elliot Zuckerberg, informatico e imprenditore statunitense, noto per essere uno dei fondatori del social network Facebook. Insieme ai suoi compagni di corso, studenti dell'Harvard University (Eduardo Saverin, Andrew McCollum, Dustin Moskovitz e Chris Hughes) Zuckerberg creò Facebook in una stanza del dormitorio di Harvard, per poi trasferirsi a Palo Alto in California.

[240] NetBlocks è un'organizzazione di vigilanza che monitora la sicurezza informatica e la governance di Internet. Il servizio è stato lanciato nel 2017. Pubblica report originali sulla

L’azienda pur non fornendo alcuna spiegazione ufficiale in un tweet ha ammesso il grave disservizio: «Siamo consapevoli che alcune persone hanno problemi ad accedere alle nostre app e ai nostri prodotti. Stiamo lavorando per riportare le cose alla normalità il più rapidamente possibile e ci scusiamo per gli eventuali disagi».

Il black out ha avuto ripercussioni anche sulla Borsa e il patrimonio personale di Zuckerberg nel giro di qualche ora sarebbe diminuito di alcuni miliardi di dollari.

Sembra escludersi la pista di un attacco hacker, in questo caso. Pare che il problema riguardasse il Dns, il Domain Name System. In pratica è come se Facebook avesse oscurato l’indirizzo con cui gli utenti potevano rintracciarlo online. Sembra che l’indirizzo www.facebook.com sia saltato dopo un aggiornamento, come non fosse mai esistito.

Una situazione, quella di Facebook, la creatura di Mark Zuckerberg, piuttosto preoccupante[241], in quanto è ormai chiaro come l'azienda soffra di gravi problemi di comunicazione al suo interno[242] e lo stesso Zuckerberg ha ufficializzato ad ottobre scorso il cambio di denominazione della popolare piattaforma social a cui ha dato il nome di Meta.

È’ stato Snapchat[243]il social che ha beneficiato più di tutti del blackout di Facebook. L’app, secondo i dati di SensorTower, condivisi con Bloomberg, ha registrato un aumento del tempo speso sulla piattaforma pari al 23%, Telegram del 18%, Signal è cresciuto del 15%. Twitter ha visto un aumento dell’11% e Tik tok del 2%[244]. Intanto, l'ex presidente degli Stati Uniti, Donald Trump, va avanti con il suo progetto della app 'Truth Social' che presenta caratteristiche simili agli strumenti di connessione online di Facebook. Trump era stato estromesso da Twitter, Facebook e YouTube dopo l'assalto a Capitol Hill il 6 gennaio 2021. Successivamente, promise che avrebbe lanciato una sua piattaforma, alternativa.

---

governance di Internet e sull'energia sostenibile, fornendo strumenti al pubblico per osservare possibili blocchi di Internet e stimare le conseguenze economiche delle interruzioni della rete.

[241] LA REPUBBLICA, *Abusi e monopolio la grande crisi di Facebook oltre il black out*, di Federico Rampini, 6 ottobre 2021, p.19.

[242] LA REPUBBLICA, *I guai della galassia Zuckerberg. Fb e Whatsapp bloccati per ore*, di Raffaella Menichini, 5 ottobre 2021, p. 20.

[243] Snapchat, un'applicazione multimediale per smartphone e tablet ideata da tre studenti dell'Università di Stanford, nel settembre 2011. La caratteristica principale di Snapchat è consentire agli utenti della propria rete di inviare messaggi di testo, foto e video visualizzabili solo per 24 ore.

[244] CORRIERE DELLA SERA, *Blackout di Facebook sale Snapchat*, 7 ottobre 2021, p.16.

3.3 - La sicurezza della rete: violato il sistema informatico dell'Europarlamento

La connessione wi-fi è stata interrotta al Parlamento europeo dopo l'assalto di alcuni hacker che sono riusciti a rubare le password delle email di alcuni deputati europei e dei loro collaboratori, accedendo all'interno della loro posta elettronica. È avvenuto nel 2013 quando per impedire atti di spionaggio, gli esperti della sicurezza del Parlamento europeo, in via cautelativa, hanno disposto la chiusura della rete wi-fi pubblica -fino a nuovo avviso - ed hanno chiesto ai deputati di scaricare sui propri smartphone un software particolare per poter accedere ai sistemi informatici del Parlamento tramite una rete wi-fi "privata":

Scriveva così l'agenzia giornalistica Ansa da Bruxelles il 25 novembre 2013: «*Rete Wi-Fi spenta al Parlamento europeo dopo l'attacco di un hacker che è riuscito a recuperare le password delle caselle e-mail di alcuni eurodeputati e collaboratori, introducendosi all'interno della loro corrispondenza privata. Per precauzione, i tecnici dell'Europarlamento hanno deciso di spegnere la rete Wi-Fi pubblica "fino a nuovo avviso" e hanno chiesto ai deputati d'installare sui propri dispositivi mobili uno specifico software per avere accesso ai sistemi informatici dell'istituzione Ue attraverso un'altra rete Wi-Fi 'privata'. A medio termine, il Parlamento intende adottare "misure aggiuntive" per rafforzare la sicurezza del sistema informatico. "Sono in corso indagini per conoscere cause e autori dell'attacco hacker", hanno fatto sapere dall'Europarlamento*».

Nel 2020, invece, quello che poteva sembrare un sistema inviolabile si è rivelato fragile ed è stato colpito da un gruppo di pirati informatici che hanno violato anche decine di mailbox di funzionari ed europarlamentari.

Un maxi data breach con informazioni relative a migliaia di dipendenti e membri dell'Europarlamento esposte in quella che Marcel Kolaja[245], vice president for IT policy del Parlamento europeo, ha definito una "grave violazione dei dati".

[245] Marcel Kolaja , ingegnere e politico ceco. È vicepresidente del Parlamento Europeo dal luglio 2019. È iscritto al Partito Pirata Ceco e fa parte del gruppo Verdi/ALE. Kolaja si era impegnato come attivista contro l'introduzione di una legge europea sul brevetto software già a partire dal 2003 e si è iscritto al Partito Pirata Ceco nel 2010. Nel 2011 è stato copresidente dell'Internazionale dei Partiti Pirata.

I dati includono 1.200 account di deputati e funzionari dell'Europarlamento, più altri 15.000 account di professionisti che lavorano per le istituzioni Ue. Le informazioni esposte comprendono dati sensibili e password crittografate e sono state sottratte da un sistema che era stato gestito sotto il dominio ufficiale "europarl.eu" del Parlamento europeo, anche se i dati erano conservati presso terzi. Si sarebbe trattato di un database contenente indirizzi e-mail e password, ma ormai ritenuto obsoleto che conteneva solo informazioni utilizzate da persone iscritte al vecchio sito web nel 2018, con collegamenti a partiti e istituzioni politiche, inclusi membri di agenzie e autorità dell'Ue come l'Europol, Frontex, il Garante privacy Edps (European data protection supervisor), utenti della Commissione europea e altri ancora.

Nel 2021 l'allora presidente del Parlamento europeo David Sassoli[246] parlando di sicurezza informatica ha affermato che «*L'UE è vulnerabile e subisce attacchi hacker quotidiani da entità governative straniere*»[247].

La mattina del 7 aprile 2021, una minaccia informatica fa scattare i protocolli di sicurezza del Parlamento Europeo. In una mail del servizio di sicurezza si legge che nelle ore passate è stato necessario ricorrere a delle «*contromisure per proteggere il sistema*». Il 12 aprile arriva un secondo allarme e a tutti i dipendenti viene chiesto di cambiare password entro 10 giorni. La spiegazione di tale richiesta sta nel fatto che, a causa dei frequenti accessi da remoto dell'ultimo anno, questa misura si è resa necessaria per garantire lo svolgimento in sicurezza di tutte le operazioni a distanza.

Pochi giorni dopo, in realtà, si scoprirà che i server adibiti alle conferenze e al lavoro da remoto hanno subito un incidente informatico con una minaccia non meglio specificata.

Secondo i tecnici le applicazioni non sono state compromesse e nemmeno i dati personali dei dipendenti sembravano essere trafugati, eppure si suggeriva di cambiare immediatamente password e di passare all'autenticazione a due fattori.

Dopo alcuni giorni i tecnici del Parlamento Europeo hanno fatto sapere che il sistema di sicurezza ha retto alla minaccia e che non ci sono stati furti o accessi indesiderati.

[246] Giornalista professionista dal 1986, è stato vicedirettore del TG1 dal 2006 al 2009. Eletto parlamentare europeo del Partito Democratico per tre mandati consecutivi, è stato Presidente del Parlamento europeo dal 2019 fino al giorno della sua morte, avvenuta l'11 gennaio scorso.

[247] https://www.eunews.it/2021/05/14/sicurezza-informatica-sassoli-lue-e-vulnerabile-e-subisce-attacchi-hacker-quotidiani-da-entita-governative-straniere/150037

Aggiungendo, però, la raccomandazione di usare l'app nativa per accedere alla mail istituzionale oltre al già citato riconoscimento a due fattori.

Non è ancora chiaro, tuttavia, se questo attacco abbia interessato gli account di posta elettronica dei deputati, quelle del loro staff, quelle dell'amministrazione o altro. Non è chiara nemmeno la natura della minaccia che, seppur sventata tempestivamente, resta comunque un grave attacco a uno degli organi strategici, cuore pulsante delle istituzioni europee.

3.4 UE: il processo di digitalizzazione e il sostegno alla ripresa nel corso dell'emergenza sanitaria

Nel corso dell'emergenza sanitaria ancora in corso, l'UE e i suoi Stati membri hanno collaborato per mitigare e contenere gli effetti dell'epidemia da coronavirus e aiutare l'Europa a superare la crisi economica. Alcuni settori critici come trasporti, energia, sanità o finanza dipendono sempre di più dalle tecnologie digitali per cui la pandemia ha impresso un'accelerazione al processo di digitalizzazione evidenziando chiaramente tutti i rischi legati alla cybersicurezza.

Mai come in questa fase si è compreso quanto sia importante anzi, indispensabile puntare su alti livelli di cybersicurezza. La UE, sulla base dell'EU Cybersecurity Act[248], mira a raggiungere un elevato livello in tutti i Paesi europei promuovendo innovazione, cooperazione e sostegno sia nel pubblico, sia nel privato.

Per questo la Commissione europea ha presentato la nuova strategia per la cybersicurezza come parte essenziale della transizione digitale, del piano per la ripresa europea e della strategia per l'Unione della sicurezza ed ha avanzato proposte relative alla resilienza informatica e fisica delle entità e delle reti critiche.

Le iniziative promosse comprendono un cyberscudo europeo (Cyber-Shield europeo) costituito da centri operativi di sicurezza, un'unità congiunta per il ciberspazio che racchiuda tutte le comunità operanti nel settore, soluzioni per rafforzare la sicurezza di Internet a livello mondiale, un regolamento per garantire un'Internet delle cose sicure. Infine, un insieme di strumenti per la diplomazia informatica ed una cooperazione rafforzata nell'ambito della cyberdifesa. Ma non solo: attivati anche un programma d'azione ONU in materia di sicurezza internazionale nel ciberspazio, importanti dialoghi a livello informatico con i Paesi terzi, nonché con la NATO e un'agenda UE per lo sviluppo delle capacità informatiche esterne.

Come abbiamo avuto modo di constatare attraverso un'esamina precedente, la strategia europea, basata sull'Agenda europea sulla sicurezza 2015-2020, ha proposto sicuramente un nuovo orientamento e un approccio coordinato ai diversi filoni della politica

[248] https://www.europarl.europa.eu/italy/it/succede-al-pe/la-nuova-strategia-europea-per-rafforzare-la-sicurezza-informatica

di sicurezza, per garantire che l'UE possa rispondere al panorama di escalation delle minacce sempre più pervasive ed in rapida evoluzione.

Anche per il sostegno alla ripresa contro l'impatto economico e sociale della pandemia molte sono le iniziative messe in campo. È stato concordato un fondo straordinario da 750 miliardi di euro, denominato Next Generation EU con priorità agli investimenti nel passaggio al digitale e nella transizione verde. Una cifra che va ad aggiungersi ai 1100 miliardi di euro del bilancio Ue rafforzato per il 2021-2027. Per un totale complessivo di 1850 miliardi. Il piano presenta in primo piano una transizione digitale accompagnata dalla strategia per la cybersicurezza, che punti anche ad un'autonomia europea in un settore considerato particolarmente strategico.

Il Parlamento europeo ha approvato poi alcuni programmi specifici, come Digital Europe, che stanza 1.7 miliardi per questo settore, prevendendo la realizzazione di un centro di competenza a Bucarest. Anche il Fondo Europeo per la Difesa, dotato di 8 miliardi, viene utilizzato per realizzare infrastrutture fisiche per la cybersicurezza e sostenere lo sviluppo tecnologico e l'innovazione.

Quattro vaccini contro la COVID-19 sono già stati autorizzati nell'UE e le vaccinazioni sono iniziate il 27 dicembre 2020 in tutta l'Unione[249].

L'UE ha coordinato uno sforzo congiunto per assicurare la produzione nell'UE di un quantitativo sufficiente di vaccini sicuri ed efficaci attraverso accordi preliminari di acquisto con i produttori ed ha firmato otto accordi con sviluppatori di vaccini per garantire fino a 4,6 miliardi di dosi.

Per consentire l'accesso ai vaccini anche da parte dei paesi a basso e medio reddito nel mondo, l'UE ha sostenuto l'iniziativa globale COVAX in materia di vaccini nell'ambito dell'approccio Team Europa. L'UE ha inoltre messo a disposizione attrezzature mediche tramite la creazione di scorte europee comuni di dispositivi di protezione individuale e ventilatori nell'ambito di rescEU.

È stato proposto anche un nuovo programma EU4Health rafforzato, che migliorerà il sostegno ai sistemi sanitari degli Stati membri, concepito per contribuire in modo

[249]https://www.consilium.europa.eu/it/policies/coronavirus/covid-19-research-and-vaccines/#:~:text=Le%20vaccinazioni%20contro%20la%20COVID,UE%20sono%20tre%20su%20quattro.

significativo alla ripresa post COVID-19 e per rafforzare la resilienza dei sistemi sanitari promuovendo l'innovazione nel settore sanitario.

Per attenuare i rischi di disoccupazione nello stato di emergenza anche uno strumento europeo di sostegno temporaneo (SURE) che fornisce agli Stati membri fino a 100 miliardi di euro di prestiti a condizioni favorevoli. Convogliati circa 37 miliardi di euro dai fondi strutturali dell'UE agli Stati membri.

Agevolato l'invio tramite il Corpo medico europeo in uno spirito di solidarietà. Austria, Lussemburgo, e Germania hanno messo le loro unità di terapia intensiva a disposizione del Belgio, Paesi Bassi, Francia e Italia. La Polonia, la Romania e la Germania hanno inviato squadre di medici per dare un contributo alla cura di pazienti negli ospedali italiani. L'Ungheria e i Paesi Bassi hanno inviato ventilatori in Repubblica Ceca. La Francia, invece, ha condiviso dosi di vaccino con la Cechia e la Slovacchia.

In Italia, nel contesto dell'emergenza epidemiologica, diversi sono gli interventi normativi con dirette implicazioni sulla protezione dei dati personali[250].

Si segnalano in particolare:

il decreto-legge 17 marzo 2020, n. 18 (cd. Cura Italia), convertito con l.24 aprile 2020, n. 27, il cui art. 17-bis, contenente disposizioni sul trattamento dei dati personali. La norma mira a garantire l'efficacia delle misure di protezione dall'emergenza sanitaria e assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale. Il provvedimento consente ai soggetti incaricati della gestione dell'emergenza, per motivi di sanità pubblica, di effettuare i trattamenti di dati personali anche sensibili o giudiziari (di cui agli artt. 9 e 10 del RGPD), mediante reciproco scambio di informazioni che risultino necessarie per l'espletamento delle funzioni.

Il decreto-legge 30 aprile 2020, n. 28 in materia di intercettazioni di conversazioni e comunicazioni, di ordinamento penitenziario e di giustizia civile, amministrativa e contabile, nonché per l'introduzione del sistema di allerta Covid-19, convertito dalla legge 25 giugno 2020, n. 70. In particolare, l'art. 6 disciplina il trattamento di dati personali nel contesto dell'emergenza sanitaria determinata dalla diffusione del Covid-19 per finalità di allertamento delle persone che possono avere avuto contatti ravvicinati con altri soggetti

[250] V. https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html

positivi al virus. Il trattamento dei dati riguarda il tracciamento effettuato tramite l'utilizzo di un'applicazione (cosiddetta Immuni), installata su base volontaria per la registrazione dei soli contatti tra soggetti che l'abbiano volutamente scaricata per adottare misure di prevenzione sanitaria nel caso si entri in contatto con utenti contagiati.

La norma, sottoposta all'esame formale del Garante, è stata modificata dall'art. 2, d.l. 125/2020, per consentire l'utilizzo del sistema di allerta anche oltre frontiera, come componente di una strategia europea di controllo del contagio del virus e di tutela della popolazione.

Il decreto-legge 10 maggio 2020, n. 30, su misure urgenti in materia di studi epidemiologici e statistiche sul Sars-Cov-2, convertito dalla legge 2 luglio 2020, n. 72. Il decreto, composto da un unico articolo, al fine di disporre con urgenza di studi epidemiologici e di statistiche sullo stato immunitario della popolazione, "autorizza" il trattamento di dati personali, anche genetici e relativi alla salute, per fini statistici in un'indagine di sieroprevalenza condotta congiuntamente dagli uffici del Ministero della salute e dall'Istat che si avvalgono di una piattaforma informatica istituita presso il Ministero.

Rispetto agli orientamenti e alle iniziative assunti in sede europea sui sistemi di tracciabilità, la Commissione europea ha adottato, invece, la Raccomandazione (UE) 2020/518, dell'8 aprile 2020[251], ossia strumenti per l'uso della tecnologia e dei dati per contrastare la crisi Covid-19 in particolare, per le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità. Il 16 aprile 2020, la Commissione ha emanato una comunicazione sugli "*Orientamenti sulle app a sostegno della lotta alla pandemia per la protezione dei dati*" C(2020)124).

Il Comitato europeo per la protezione dei dati (EDPB), invece, il 21 aprile 2020 ha pubblicato le Linee guida[252] sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nell'ambito dell'emergenza. Nel documento viene stabilito che la disciplina europea sulla protezione dei dati reca «*norme specifiche che consentono l'uso di dati anonimi o personali per sostenere le autorità pubbliche e altri soggetti, a livello nazionale e dell'UE, nel monitoraggio e nel contenimento della diffusione del virus SAR-*

[251] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32020H0518

[252]https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_it

CoV-22». *L*'utilizzo degli strumenti previsti per il tracciamento dei contatti «*dovrebbe essere volontario e non basarsi sulla tracciabilità dei movimenti individuali ma sulle informazioni di prossimità relative agli utenti*».

Il 13 maggio 2020 gli Stati membri[253], con il sostegno della Commissione europea, hanno stabilito gli orientamenti per l'interoperabilità transfrontaliera delle applicazioni di tracciamento, nella sede dell' eHealth Network, una rete che unisce le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri, istituita sulla base dell'articolo 14 della direttiva 2011/24/UE del Parlamento europeo e del Consiglio (2011), sull'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.

Si prevede che nei prossimi anni i criminal hacker saranno impegnati in attacchi informatici sempre più pericolosi e sofisticati.

Nel contempo, però, la maggiore incidenza e intensità delle minacce dimostra che l'attuale quadro legislativo non è adeguato allo scopo. Dalla valutazione dell'attuazione della direttiva NIS è emerso, come abbiamo visto nei precedenti capitoli, che il suo ambito di applicazione non rispecchia il livello attuale di digitalizzazione e interconnessione, né l'interdipendenza di settori economici e sociali fondamentali.

Nel dicembre 2020 la Commissione ha pertanto proposto due importanti atti legislativi: una direttiva sulla resilienza dei soggetti critici (CER) e una direttiva rivista relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS rivista)[254].

La trasformazione digitale resta una delle priorità dell'UE dal momento che il Parlamento europeo è impegnato nel rafforzare le tecnologie digitali, in nuove opportunità per aziende e consumatori e nel consentire la transizione verde della Ue e la neutralità carbonica entro il 2050 ma anche nella formazione digitale per cittadini e servizi pubblici.

[253] https://ec.europa.eu/health/ehealth/covid-19_it

[254] Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

In sostanza la Commissione ha presentato nella prima metà dei 2020 in tema di digitalizzazione:

La strategia industriale;

La strategia per le PMI;

Il Libro Bianco sull'Intelligenza Artificiale;

La Strategia europea per i dati.

La Strategia industriale europea, accompagnata da quella per le PMI propongono entrambe di attuare la transizione digitale e sostenibile attraverso una riduzione della burocrazia e un accesso facilitato ai numerosi fondi pubblici a disposizione delle imprese. Accanto a Horizon 2020 (il fondo per l'innovazione più importante), è stato proposto un Digital Europe Programme,

un programma da 7,5 miliardi di euro che punta a rafforzare l'autonomia dell'Unione in cinque ambiti di intervento che l'UE considera strategici: tre tecnologie, ossia high performance computing, Intelligenza Artificiale (IA) e cyber security; le digital skill e più nello specifico la costruzione delle tecnologie avanzate necessarie per l'indipendenza dell'Unione in questi ambiti; infine, la promozione di best practice sull'utilizzo delle tecnologie strategiche. L'intelligenza artificiale può migliorare il livello di vita delle persone e portare ingenti vantaggi alle aziende europee in campo sanitario, in settori come l'economia verde e circolare, la meccanica, l'agricoltura, il turismo e molti altri.

Inoltre, è stato previsto un fondo specializzato per le PMI e l'iniziativa ESCALAR servirà ad attirare più investimenti privati. Verrà invece concessa alle aziende consulenza strategica e digitale da parte dei cosiddetti Poli dell'innovazione digitale mentre il programma CEF (Connecting Europe Facility), si occupa di promuovere investimenti nelle infrastrutture strategiche, come banda larga e 5G.

Creative Europe, è il programma dedicato all'industria creativa e ai media e EU4Health, agli investimenti nella digitalizzazione del settore sanitario.

Con la Bussola Digitale, invece, la Commissione europea ha presentato una visione, obiettivi e percorsi per realizzare la trasformazione digitale dell'Europa entro il 2030, una

strategia chiave per completare anche la transizione verso un'economia sostenibile e resiliente.

La strategia di trasformazione digitale del settore agricolo, invece, punta a sfruttare i Big Data per la politica agricola comune (CAP) mentre Recovery and Resilient Facility (RRF), mette a disposizione un totale di 723,8 miliardi di euro per la ripresa degli Stati membri dopo la pandemia.

Lo strumento di finanziamento per stimolare gli investimenti europei è quello InvestEU, il cui quadro di riferimento è il MFF (Multiannual Financial Framework), ossia il bilancio pluriennale dell'UE, che delinea le strategie e le risorse disponibili per il periodo 2021-2027.

Il piano per rilanciare l'economia richiede agli stati membri di investire almeno il 20% dei 672.500 milioni di euro del Dispositivo per la ripresa e la resilienza nel settore digitale. Anche i programmi di investimento come Orizzonte Europa per l'innovazione e il Fondo per collegare l'Europa per l'infrastruttura investono grandi somme per l'avanzamento del digitale.

In Italia, il tema della cybersecurity è particolarmente di attualità all'interno del piano Industria 4.0. L'adeguamento alla versione 4.0 della sicurezza richiede l'individuazione delle difese dei sistemi da problemi interni ma anche da attacchi esterni. Quest'ultimo aspetto trae origine non solo dalla politica e dal livello di sicurezza dell'impresa, ma anche dalla sicurezza dell'ambiente di rete e d'infrastruttura. Nato come Industria 4.0 è poi divenuto Impresa 4.0 e, ormai, dal 2020 Transizione 4.0, un piano italiano a sostegno degli investimenti nelle tecnologie abilitanti per la quarta rivoluzione industriale[255].

Il Dipartimento per la trasformazione digitale (Dtd), alla fine del 2021, ha dato il via alla gara per il Cloud nazionale della Pubblica Amministrazione[256] e ha indicato la proposta del raggruppamento di imprese guidato da Tim, Cdp Equity, Leonardo e Sogei come quella di riferimento per poter permettere l'avvio dei lavori entro la seconda metà del 2022.

---

[255] A. LIOTTA, *Una spinta verso la trasformazione tecnologica delle imprese: l'iperammortamento come strumento di politica fiscale per l'innovazione*, Luiss Law Review, 2017, p. 145.

[256]https://innovazione.gov.it/notizie/articoli/cloud-pa-selezionato-il-progetto-psn-gara-prevista-nelle-prossime-settimane/

Il Piano Nazionale di Ripresa e Resilienza (Pnrr) prevede infatti, la creazione di un'infrastruttura innovativa per abilitare e accelerare il processo di migrazione verso il Cloud dei servizi e dei dati delle P.a. centrali e locali, il cosiddetto Polo Strategico Nazionale (Psn).

Per la realizzazione del Piano Strategico Nazionale è stata prevista un'iniziativa da realizzarsi con il contributo essenziale di partner privati, mediante lo strumento del Partenariato Pubblico-Privato.

L'obiettivo è supportare le amministrazioni in questo processo e offrire i più elevati standard di sicurezza per il trattamento di dati e servizi critici e strategici per il Paese[257].

[257]https://innovazione.gov.it/notizie/articoli/cloud-pa-selezionato-il-progetto-psn-gara-prevista-nelle-prossime-settimane/

3.5 Strategie e modelli organizzativi per le imprese

Il problema delle minacce informatiche concerne sia le piccole e medie imprese (PMI) sia le multinazionali poiché frutto della congiuntura su scala internazionale, determinata oggi dallo stato di emergenza sanitaria e dall'affermazione di scenari riferibili al cyberwarfare.

L'attuazione di strategie e di modelli organizzativi prevengono il rischio della perdita dell'integrità e della confidenzialità dei dati e delle informazioni, impedendo o rendendo più complicato portare a compimento reati a livello informatico.

Per questo è importante implementare un modello organizzativo aziendale per la cybersecurity, calibrato sulle esigenze di business della società nel rispetto delle disposizioni normative sulla sicurezza informatica Davanti all'aumento di violazioni di alto rilievo, a inverosimili perdite di dati e attacchi ransomware, molte organizzazioni non hanno il budget per creare o subappaltare un programma di sicurezza informatica (InfoSec) e sono quindi costrette a imparare sul campo[258].

La Direttiva 1148/2016 (NIS), il Regolamento UE 679/2016 (GDPR) e il D.L. 105/2019 sul Perimetro di Sicurezza Nazionale[259] Cibernetico e l'approccio stesso del legislatore rivelano una maggiore sensibilità nei confronti della cybersecurity e rivelano quanto essa sia rilevante sotto un profilo tecnologico, umano e organizzativo per attuare e formalizzare quelle misure necessarie per mitigare i fattori di rischio sugli asset aziendali. Consentono insomma. di diffondere una visione multidisciplinare della sicurezza informatica. L'approccio del legislatore è indirizzato verso un percorso di responsabilizzazione e, di conseguenza, verso la scelta di misure di sicurezza più efficaci ed efficienti per difendersi dagli attacchi informatici.

[258] V. L. BROTHERSTON, A. BERLIN, R. VISCARDI (Traduttore), *La sicurezza dei dati e delle reti aziendali. Tecniche e best practice per evitare intrusioni indesiderate*, O'Reilly, 2018.

[259] Decreto legge 21 settembre 2019, n. 105 contenente «*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*». mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza per minimizzare i rischi.

Del resto, la sicurezza informatica si basa su 3 elementi cardine che costituiscono una triade meglio conosciuta con l'acronimo CIA: Confidentiality, Integrity e Availability.

• Confidentiality (Confidenzialità): consiste nella abilità di proteggere i dati da accessi non autorizzati: la crittografia e l'introduzione di rigidi criteri per l'autenticazione come password complesse o l'impostazione di una data di scadenza minima. La confidenzialità deve essere assicurata lungo tutte le fasi di vita del dato, dal suo inserimento, al suo utilizzo, al suo transito lungo la rete di connessione.

Le cause di violazione della confidenzialità possono essere imputabili ad un attacco malevolo oppure ad un errore umano.

• Integrity (Integrità): consiste nell'essere in grado di proteggere le informazioni da modifiche o cancellazioni indesiderate. Nei sistemi devono essere implementati vari livelli autorizzativi che presentino, a seconda della profilazione e del ruolo dell'utente, diverse autorizzazioni ad agire sui sistemi.

È la abilità di conservare la veridicità dei dati e delle risorse e assicurare che non vengano modificate o cancellate, ad opera di soggetti non autorizzati. L'integrità può riferirsi a situazioni diverse come prevenire le modifiche non autorizzate ad informazioni da parte degli utenti, oppure garantire che le informazioni siano identificabili e verificabili.

• Availability (Disponibilità): è la capacità di permettere un accesso sicuro ai dati in caso di necessità di fronte a problemi causati da guasti, errori, blackout o cancellazione di dati a causa di attacchi DDoS.

Per conservare un elevato grado di disponibilità delle informazioni possono risultare utili sistemi di backup remoto, ridondanza di archivi, firewall e gruppi di continuità.

Rendere un servizio disponibile significa infatti, impedire che avvengano interruzioni di servizio e garantire che le risorse infrastrutturali siano pronte per la corretta erogazione.

Esistono anche altre ragioni, oltre a quelle di origine dolosa, che possono generare una violazione di disponibilità, come ad esempio il sovrautilizzo di componenti hardware e software oppure una rimozione di dati accidentale.

Sicuramente il progresso delle tecnologie informatiche ha reso difficile in questi anni, trovare una soluzione statica capace in assoluto di evitare e contrastare gli attacchi informatici.

Per questo occorrono soluzioni all'avanguardia e sempre aggiornate con i migliori prodotti di hardware, software, antivirus e strumenti tecnologici.

Ogni società deve individuare quelli che sono i "punti deboli" dei propri sistemi informativi studiando i processi, analizzando le minacce e valutando il livello di difesa. Fondamentale è la conoscenza del pericolo per potersi difendere dopo una analisi particolareggiata ed attente delle minacce e dei mezzi con cui si diffondono.

Il Decreto Legislativo 8 giugno 2001, n.231 in Italia ha introdotto la responsabilità amministrativa delle persone giuridiche[260], delle società e delle associazioni anche quelle prive di personalità giuridica in attuazione dell'art.11 della Legge-delega n.300 del 2000.

In questo modo il legislatore ha voluto ratificare le Convenzioni internazionali, con riferimento alla Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, alla Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e alla Convenzione Ocse del 17 dicembre 1997 contro la corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto legislativo, che delinea un vero e proprio microcodice, qualifica la responsabilità degli enti come amministrativa.

Tuttavia in dottrina e in giurisprudenza si sono registrati orientamenti differenti.

Secondo una prima tesi[261], che muove dal criterio utilizzato dal legislatore per definire la responsabilità dell'ente, qualifica quest'ultima come amministrativa adducendo una serie di argomentazioni.

In primo luogo, il principio di colpevolezza evoca la presenza di elementi psichici assenti all'interno di enti collettivi.

Inoltre il finalismo rieducativo della pena di cui all'art 27 comma 3 della Costituzione riguarderebbe soltanto la persona fisica e non anche le organizzazioni complesse.

A questo orientamento se ne aggiunge un altro[262] che invece sostiene la natura penale della responsabilità dell'ente, in virtù del fatto che i criteri di imputazione consentono di muovere un rimprovero personale, con la conseguenza che l'ente responsabile sarà chiamato a rispondere per un fatto proprio e colpevole.

---

[260] G. LATTANZIO, P. SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol.II, Diritto processuale, G.Giappichelli editore, 2020, p.7

[261] I. CARACCIOLI, *I soggetti del diritto penale: evoluzione delle categorie dagli anni Cinquanta ad oggi,* in dir.pen. XXI secolo,2005, p.6

[262] A. CARMONA, *Premesse a un corso di diritto penale dell'economia*, Cedam, 2002, p.208

Un terzo orientamento[263] invece qualifica la responsabilità dell'ente come un tertium genus, ossia un ibrido che consente di conciliare elementi dell'illecito penale e dell'illecito amministrativo.

Le Sezioni Unite[264] hanno inoltre affermato che la disciplina punitiva ex d.lgs.231/2001 sarebbe compatibile con l'art 27 della Costituzione[265]: il primo comma infatti evoca il principio di personalità della responsabilità, e si evidenzia che il reato della persona fisica si considera proprio dell'ente in virtù del rapporto di immedesimazione organica .

Anche l'art 27 comma 3 sarebbe rispettato in quanto il decreto prevede che la sanzione pecuniaria sia comminata per quote e adeguata alla capacità economica dell'ente. prevede, in riferimento ad alcune specifiche fattispecie, una responsabilità amministrativa degli Enti che è paragonabile alla responsabilità penale.

La responsabilità amministrativa dell'ente si aggiunge a quella della persona fisica che ha commesso materialmente il reato. Tale responsabilità viene meno se si dimostra di aver istituito un Organismo di Vigilanza e di aver adottato modelli organizzativi specifici al fine di prevenire la commissione di reati.

Nel 2001 i reati informatici non erano contemplati in questa normativa, (vi era solo il reato di "frode informatica a danno di enti pubblici") e quindi, nel 2008, hanno fatto il loro ingresso a seguito della Legge 48/2008 che ha ratificato la Convenzione di Budapest del Consiglio d'Europa sul cyber crime apportando alcune modifiche al codice penale e a quello procedurale penale e di conseguenza al D.lgs. 231/01.

Il decreto legislativo 231/2001 introduce nel nostro ordinamento la responsabilità amministrativa degli enti dipendente da reato[266] e rappresenta sicuramente un'innovazione legislativa rilevante, poiché di fatto sancisce il superamento del principio «societas

[263] In tal senso v. Cass.,18 febbraio 2018, n.27735; Cass.,9 luglio 2009, n.36083.

[264] In questa direzione, Cass., Sez.Un, 18 settembre 2014, n.38343, in Società,2015, p.215 ss.

[265] Nella Parte I "Diritti e doveri dei cittadini" – Titolo I (Rapporti civili), l'articolo 27 della nostra Costituzione sancisce che la responsabilità penale è personale.

[266] Art. 1 d.lgs. 231/2001: «*Il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale*».

delinquere et puniri non potest», privilegiando un'esigenza di razionalizzazione della normativa alla luce dell'esistenza di un'evidente potenzialità criminale delle persone giuridiche.

Questo ovviamente ha suscitato pensieri della dottrina giuridica spesso non omogenei ed è questo il motivo per cui coesistono spesso definizioni di "responsabilità amministrativa degli enti" e di "responsabilità penale degli enti" in rapporto al decreto di cui trattasi.

Questa responsabilità per l'Ente riguarda i reati posti in essere da soggetti che si trovano in posizione apicale (art. 5 c.1 lett. a) o sottoposti alla direzione di un apicale (art. 5 c.1 lett. b), per illeciti condotti nell'interesse e/o a vantaggio dell'ente ove interesse e vantaggio sono da classificarsi come due condizioni indipendenti anche se non necessariamente coesistenti.

È importante aggiungere che, se il reato viene commesso da un soggetto in posizione apicale la colpa dell'ente è presunta mentre nel caso di commissione da parte di un soggetto sottoposto, l'ente sarà ritenuto responsabile ove l'illecito sia stato reso possibile dall'inosservanza degli obblighi di direzione o vigilanza.

L'ente è ritenuto responsabile per i reati commessi, dai soggetti apicali o subordinati[267] solo se gli illeciti vengano commessi nel suo interesse o a suo vantaggio[268].

Per evitare una distorsione del principio «*nulla poena sine culpa*» e di costruire un'inammissibile ipotesi di responsabilità oggettiva, è prevista la sussistenza della cosiddetta "colpa di organizzazione".

Il legislatore ha voluto imporre agli enti l'obbligo di adottare iniziative di carattere organizzativo e gestionale[269]. Questi accorgimenti specifici devono essere consacrati in un documento, un modello che individua i rischi e definisce le misure per evitarli.

---

[267] Art. 5 comma 1 lett. a) e b) d.lgs. 231/2001: «*Per soggetti apicali si intende: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso. E per subordinati: persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra*».

[268] Art. 5 comma 2 d.lgs. 231/2001: «*L'ente non risponde se i soggetti di cui sopra hanno agito nell'interesse esclusivo proprio o di terzi*».

[269] Art. 6 d.lgs 231/2001: «1.*Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un*

Non aver ottemperato a tale obbligo consente l'imputazione a carico dell'ente dell'illecito amministrativo dipendente da reato. L'accusa ha l'onere di dimostrare l'esistenza dell'illecito penale in capo alla persona fisica che fa parte della compagine organizzativa della societas e che abbia agito nell'interesse di questa; questa responsabilità accertata si estende dall'individuo direttamente all'ente collettivo ed è onere dell'ente provare, per contrastare gli elementi di accusa posti a suo carico, le condizioni liberatorie di segno contrario di cui all'articolo 6 del decreto legislativo 231 del 2001.

Gli artt. 6 e 7 d.lgs. n.231 incentrano la responsabilità sull'adozione di modelli di organizzazione e gestione «*idonei a prevenire reati della specie di quello verificatosi*». ciò significa che il reato della persona fisica costituisce solo il presupposto ma non l'oggetto della responsabilità, che è fondato su una colpa di organizzazione dell'ente legata all'omissione di misure atte a impedire quel tipo di reati[270].

Il modello richiede la creazione di un organismo interno di vigilanza, che si atteggia come uno strumento informativo e di controllo.

In particolare l'organismo di vigilanza è dotato di autonomi poteri di iniziativa e di controllo e vigila sul funzionamento e l'attuazione dei modelli e ne cura l'aggiornamento. Questi, nell'espletamento delle sue funzioni, entra in contatto con una pluralità di dati personali, dati sensibili e dati giudiziari per cui questo impone di procedere all'individuazione dei pertinenti profili connessi con il trattamento dei dati personali, ai sensi del decreto legislativo 30 giugno 2003, n. 196.

I modelli organizzativi devono individuare le attività nel cui ambito possono essere commessi reati, prevedere dei protocolli per la formazione e l'attuazione delle decisioni

---

organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b). 2. In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze: a) individuare le attività nel cui ambito possono essere commessi reati; b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello».

[270] A. ALESSANDRI, S. SEMINARA, *Diritto penale commerciale*, Vol.I, I Principi generali, G. Giappichelli Editore, 2018, p.98.

dell'ente, individuare modalità di gestione delle risorse finanziarie, prevedere obblighi informativi nei confronti dell'organismo di vigilanza introducendo anche un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

La prima fase dunque si sostanzia nella mappatura del rischio, individuando tutti i settori e i processi dell'impresa in cui possano essere commessi degli illeciti.

La mappatura implica anche l'analisi normativa sia del novero dei reati presupposto che delle modalità di realizzazione degli stessi e l'identificazione di un rischio tollerabile, posto che il rischio zero non è raggiungibile.

Un altro elemento importante è rappresentato dai protocolli che alludono alla necessità di prevedere una organizzazione interna improntata allo schema della delega di funzioni, individuando una serie di soggetti preposti al controllo dei singoli settori, assicurando che tutti i processi aziendali siano sottoposti a sistemi di controllo.

La gamma di sanzioni che il dlgs 231/2001 riserva all'ente collettivo responsabile di un illecito dipendente da reato risulta piuttosto variegata.

L'art 9 prevede che possano essere irrogate nei confronti dell'ente responsabile sanzioni pecuniarie, sanzioni interdittive, la confisca e la pubblicazione della sentenza.

E' bene osservare come la legge 18 marzo 2008 n. 48[271] aveva introdotto nel catalogo dei reati presupposto del decreto legislativo 231/2001 (articolo 24 bis) diversi delitti informatici. Successivamente il decreto legge 14 agosto 2013 n. 93 ha disposto un'ulteriore integrazione dell'articolo 24 bis inserendovi alcuni delitti contenuti nel codice privacy: illecito trattamento di dati personali (articolo 167), falsità nelle dichiarazioni e notificazioni al garante (articolo 168) e inosservanza di provvedimenti del garante (articolo 170). L'art. 4 del GDPR, come abbiamo visto, definisce violazione dei dati personali (data breach) «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». Il «data breach» può aver luogo nelle tre tipologie di eventi, ossia «confidentiality breach» ossia divulgazione o accesso non autorizzato ai dati

[271] C.SARZANA DI S. IPPOLITO, *La legge di ratifica della convenzione di Budapest*, in Dir. Pen.Proc., 2008, p.1562.

personali, «availability breach», alterazione di dati personali o «integrity breach», modifica di dati personali.

La Corte di cassazione[272] ha osservato come «mentre l'aggiunta nell'elenco dei reati che fanno insorgere la responsabilità amministrativa degli enti della frode informatica e dell'indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento, non ha particolare importanza in sede applicativa, il richiamo ai delitti previsti dal codice privacy risulta di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del d.lgs 231/2001».

L'obiettivo di responsabilizzazione degli enti in relazione al corretto trattamento dei dati personali viene perseguito nel nuovo Regolamento europeo.

Il legislatore dell'Unione ha palesato una preferenza per quelle forme di responsabilità indirizzate verso la persona giuridica. Il Regolamento, infatti, prevede molte disposizioni che testimoniano la volontà di imporre gli obblighi di corretta gestione dei dati direttamente in capo alle società, rectius alle imprese. Anche le sanzioni pecuniarie di cui all'art 83 GDPR sembrerebbero prodotte in base alla capacità economica delle grandi imprese.

Le norme di disciplina del Capo IV del GDPR, prevedono obblighi gestionali e organizzativi concretizzabili soltanto all'interno di enti collettivi Un esempio è dato dalla figura del responsabile per la protezione dei dati (art 38) a cui sono attribuiti compiti di vigilanza sul rispetto della legge, consulenza, intermediazione ma anche sensibilizzazione e formazione del personale.

Il responsabile del trattamento dovrà, per impostazione predefinita, mettere in atto misure tecniche e organizzative adeguate «tenuto conto dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche» (artt 24 e 25 il livello di sicurezza e misure di protezione non è predeterminato ex ante, dovendo piuttosto essere «adeguato al rischio» (art 32 par 1 Il titolare è inoltre tenuto a effettuare una valutazione di

[272] Cass. Pen. Relazione n. III/01/2013, 22 agosto 2013.

impatto sulla protezione dei dati tutte le volte in cui il trattamento «prevedendo in particolare l'uso di nuove tecnologie può presentare un rischio elevato»

Il sistema di protezione dei dati personali sembra dunque ruotare attorno al concetto di rischio, per far fronte al quale l'impresa sarà tenuta ad implementare idonee misure di prevenzione. Inoltre, sia il D.Lgs. n. 231/2001 sia il GDPR si occupano di Whistleblowing[273]. Con il termine whistleblower si definisce il dipendente pubblico che segnala illeciti di interesse generale e non di interesse individuale e soprattutto le violazioni delle misure indicate nel modello,di cui venga a conoscenza in ragione del rapporto di lavoro, in base a quanto previsto dall'art. 54 bis del d.lgs. n. 165/2001 così come modificato dalla legge 30 novembre 2017, n. 179.

La direttiva Nis e il relativo decreto di attuazione (d.lgs. n. 65 del 2018) e il Regolamento generale sulla protezione dei dati personali hanno iniziato a disegnare un quadro normativo comune a livello eurounitario nei settori strategici, nell'ottica della cybersecurity, delle infrastrutture critiche e della data protection[274]. Essi rispondono ad una logica diversa rispetto a quella che anima il sistema previsto dal d.lgs. 231/2001.

Tuttavia, a proposito di normativa privacy e d.lgs. 231/2001 è possibile cogliere alcune importanti similitudini rispetto alla responsabilità delle persone giuridiche. L'ente sarà chiamato a rispondere dell'illecito compiuto nel suo interesse o a suo vantaggio qualora non abbia adottato e implementato le misure organizzative necessarie a contenere il rischio. Per non incorrere in responsabilità sarà tenuta ad elaborare un modello organizzativo idoneo ex art 6 del Decreto legislativo del 2001.

Preme tuttavia precisare che l'adozione di un modello organizzativo non costituisce un obbligo ma un onere tale da escludere che l'ente possa essere chiamato a rispondere del reato presupposto. In estrema sintesi, l'efficacia esimente riconosciuta all'adozione di misure di prevenzione del rischio potrebbe rappresentare un fattore comune tra i due sistemi in esame.

---

[273] V. ARAGONA, *La tutela penale della privacy nel cyberspazio,* in Rivista di diritto penale contemporaneo. Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione, Editore Associazione "Progetto giustizia penale", 2019, p.260

[274] G. LATTANZIO, P. SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol.I, diritto sostanziale, G.Giappichelli Editore, 2020, p.389

Nella prevenzione degli attacchi cibernetici, il ruolo dell'organizzazione è divenuto centrale all'insegna della cooperazione pubblico-privata che può palesarsi sotto forma di collaborazione tra autorità statali e internet service provider, di obblighi di comunicazione in capo a determinati operatori degli incidenti informatici e, infine, di adozione di misure dirette a contenere e gestire il rischio connesso alle minacce.

Sotto questo aspetto, non viene incontro solo il decreto 231 ma anche, appunto, la Direttiva Nis e il Regolamento Data Protection, ispirati alla logica dell'accountability delle imprese.

In alcuni casi non può trovare applicazione il d.lgs. n.231 del 2001[275] che, richiede la sussistenza di un reato commesso nell'interesse o a vantaggio dell'ente. In alcune ipotesi è proprio l'ente il riferimento di attacchi cibernetici.

E' possibile, a tal proposito, individuare almeno tre contesti di rilevanza[276]. In un primo caso si fa riferimento all'integrazione di reati, come l'accesso abusivo al sistema informatico e telematico, nonché all'ipotesi di intercettazione illegale. Si pensi all'accesso finalizzato a sottrarre dati sensibili di un'impresa, ad esempio una lista di clienti. La seconda ipotesi riguarda le attività di imprese che intrattengono rapporti con la PA con condotte destinate alla manipolazione dei dati come ad esempio, la modifica dei requisiti necessari per la partecipazione a gare di appalto. Infine, il danneggiamento o interruzione del funzionamento di un sistema informatico o telematico per provocare un disservizio che causi danni all'immagine societaria.

La cybersecurity è divenuta la seconda emergenza in Europa, dopo il cambiamento climatico e ancor prima dell'immigrazione. È quanto affermato dal presidente della Commissione Europea Jean-Claude Junker nel discorso sullo stato dell'Unione del 13 settembre 2017. In realtà da diversi anni paesi di tutto il mondo mettono la cybersecurity tra le priorità delle loro agende. Tra le maggiori minacce da affrontare, il blocco della

[275] V. PIERGALLINI, *I reati presupposto della responsabilità dell'ente e l'apparato sanzionatorio, in AA.VV., Reati e responsabilità degli enti*. Guida al d.lgs. 8 giugno 2001, n.231, Giuffrè, 2010, p.219.

[276] G. DEZZANI, M.L. PICCINNI, *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs.n. 231 del 2001*, in Resp.amm. soc.ed enti, 2011, Plenum, p.4.

operatività di aziende, il controllo abusivo di servizi di infrastrutture critiche, furto della proprietà intellettuale o di informazioni cruciali per la vita di un'azienda.

Le recenti campagne di malware, wannacry e notpetya, sono stati gli eventi tangibili di una serie spaventosa di attacchi in ogni angolo del pianeta.

Per questo, negli ultimi anni, si sono intensificati gli sforzi per creare nel mondo delle imprese una cultura della cybersecurity e per offrire un contributo conoscitivo sui controlli da adottare.

Primo fra tutti, il Libro Bianco[277] elaborato dal Laboratorio nazionale di Cybersecurity del Cini del 2015 per raccontare le principali sfide di cybersecurity che il nostro Paese avrebbe affrontato nei cinque anni successivi. Il volume si concentrava, soprattutto, sui rischi derivanti dagli attacchi cyber e delineava alcune raccomandazioni anche di tipo organizzativo.

Qui vengono considerati molti aspetti legati alla cybersecurity, dalla definizione di infrastrutture e centri necessari a organizzare la difesa alle azioni, alle diverse tecnologie da sviluppare per essere protetti al meglio, fino alla proposta di un gruppo di azioni per la formazione, la sensibilizzazione e la gestione dei rischi.

Emergono così le misure da adottare per contenere il rischio. In sostanza, l'ente deve definire una precisa politica di utilizzo e gestione delle password. Ai sistemi aziendali è opportuno accedere tramite apposite chiavi di accesso con l'obbligo di utilizzo delle sole postazioni aziendali con sistema di controlli e verifica dei software impiegati. Si dovrà assicurare una costante tracciabilità delle attività sulla rete e della gestione degli account di tipo amministrativo.

La legge 18 novembre 2019, n. 133, di «*Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, prevede disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*».[278] introduce un'articolata disciplina che

[277] R. BALDONI, R. DE NICOLA, P. PRINETTO, (a cura di), *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici*, Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l'Informatica, 2018, p.18.

[278] Come recita il comma 1 dell'art. 1, il provvedimento (che è entrato in vigore il 21 novembre 2019) intende «*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione,*

definisce i soggetti pubblici e privati coinvolti, i vari obblighi ed adempimenti cui sono tenuti, i rischi e le misure da adottare per fronteggiarli, i poteri di certificazione, controllo, ispezione, prescrizione delle autorità governative, le norme in materia di acquisizione e utilizzazione delle tecnologie rilevanti.

Sul piano penale introduce all'art. 1 comma 11 una nuova fattispecie che stabilisce una struttura "sanzionatoria".

Il c.11- bis dell'art.1, aggiunto a seguito di conversione del d.l.n.105/2019, inserisce le nuove fattispecie delittuose nel catalogo dei reati presupposto, la cui commissione implica la responsabilità amministrativa da reato dell'Ente, ai sensi del d.lgs. n. 231/2001.

Superata quindi, l'anomalia che emergeva dal testo del d.l. n.105/2019, in cui la responsabilità amministrativa degli enti per gli esaminati delitti era autonomamente prevista, ma senza inclusione espressa nel corpo del d.lgs. n. 231/2001.

La norma ha esteso la responsabilità dell'ente ai delitti introdotti dalla legge sul perimetro nazionale di sicurezza cibernetica che puniscono le condotte di falso che incidono sulle verifiche ispettive e/o sull'attività di controllo delle autorità preposte alla sicurezza delle infrastrutture critiche.

Nel giugno 2021, l'ENISA ha emanato il parere "Cybersecurity for SMEs[279]", con il quale intende fornire alle PMI alcuni consigli pratici in ambito di cybersecurity per consentire alle stesse di fronteggiare efficacemente i cybercrime attack che, proprio nel periodo della pandemia, hanno registrato un considerevole incremento.

E' interessante vedere come il c.d. fattore umano[280], con una formazione adeguata e regolare in favore degli operatori dell'area IT, risulti tra queste raccomandazioni insieme alla "Policy di sicurezza" sulle modalità di utilizzo dell'ambiente, delle attrezzature e dei

anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

[279] L'ENISA ha analizzato la capacità delle PMI all'interno dell'UE di far fronte alle sfide alla cibersicurezza poste dalla pandemia. La relazione fornisce consigli sulla cybersicurezza per le PMI, ma anche proposte di azioni che gli Stati membri dovrebbero prendere in considerazione per aiutare le PMI a migliorare la loro posizione in materia di cybersicurezza.

[280] L'anno in rassegna. Relazione sul Panorama delle minacce analizzato dall'ENISA. Da gennaio 2019 ad aprile 2020.

servizi ICT aziendali, da aggiornare con una cadenza regolare al momento di una effettiva necessità.

Altro elemento è il Test periodico di vulnerabilità e di sicurezza dei sistemi critici aziendali (es. firewall) insieme al controllo costante dei computer, per verificare l'eventuale presenza di software illegali o comunque non approvati.

Altri suggerimenti che possono risultare utili: proteggere sempre gli apparati informatici con sistemi antivirus aggiornati, crittografia da applicare ai dati archiviati e/o ai dati trasferiti su reti pubbliche (es. internet), protezione da accessi non autorizzati alle risorse critiche IT (es. sala server), back up regolare (e crittografato, se possibile), compreso il test di ripristino, stipulare accordi contrattuali con i fornitori ICT esterni, per regolamentare le modalità, i termini e la portata estensiva dell'accesso alle informazioni, inclusa un'apposita clausola di confidenzialità e di riservatezza.

L'ENISA ha evidenziato, quindi l'importanza di sviluppare un elenco di requisiti ed obblighi minimi di sicurezza informatica che ogni fornitore ICT[281] deve possedere affinché possa interagire con l'impresa. Sarà importante curare, con regolarità, un inventario dei propri fornitori ICT e condurre audit di sicurezza nei confronti dei fornitori insieme all'attuazione di una procedura di gestione dei dati personali trattati dal fornitore ICT, nel caso in cui il rapporto contrattuale venisse estinto.

Altri consigli da tenere nella dovuta considerazione descritti dall'ENISA: utilizzare password complesse, preferibilmente costituite dalla cd. passphrase, una raccolta di parole comuni casuali combinate in una frase che rappresenti una combinazione di memorizzazione e sicurezza; ove possibile, viene raccomandato di utilizzare l'autenticazione a più fattori (MFA) oltre all'aggiornamento, in modo regolare ed automatico, dei software.

Con la crescita dell'innovazione tecnologica e la rapida espansione del cyberspazio, politiche di cybersicurezza efficaci ed esaurienti a livello dell'UE sono di fondamentale

[281] Cyber Threat Intelligence – (CTI) sono conoscenze, competenze ed informazioni basate sull'esperienza relative al verificarsi e alla valutazione delle minacce informatiche e fisiche e degli attori delle minacce che hanno lo scopo di aiutare a mitigare potenziali attacchi ed eventi dannosi che si verificano nel cyberspazio. Le fonti di intelligence sulle minacce informatiche includono intelligence open source , intelligence sui social media , intelligence umana , intelligence tecnica, file di registro del dispositivo, dati acquisiti in modo forense o intelligence dal traffico Internet e dati derivati dal deep e dal dark web.

importanza. Forniscono la necessaria capacità di difesa a tutti i livelli della società: pubbliche amministrazioni, infrastrutture critiche, aziende, settore terziario e singoli individui. La capacità di difesa deve essere efficace e flessibile per affrontare le nuove sfide che si presentano, tenendo testa alla costante evoluzione del ciberspazio. Considerato il numero sempre crescente di portatori di interessi a livello dell'UE e degli Stati membri coinvolti in attività di questo tipo, la cooperazione e il coordinamento rispetto a queste attività in tutta l'Unione sono essenziali. I sistemi di Big Data comportano una serie di rischi per la sicurezza, stanno diventando sempre più obiettivi di attacco da parte di agenti di minaccia che con attacchi sempre più elaborati e specializzati sfruttano vulnerabilità e debolezze.

L'ampia raccolta e l'ulteriore elaborazione delle informazioni personali nell'ambito dell'analisi dei Big Data ha generato gravi problemi di privacy, in particolare in riferimento alla sorveglianza elettronica su larga scala, alla profilazione e alla divulgazione di dati privati. Per sfruttare tutti i vantaggi dell'analisi, senza tuttavia invadere la sfera privata delle persone, è importante tracciare i limiti dell'elaborazione dei Big Data e integrare le misure di protezione dei dati nella catena del valore dell'analisi[282].

Ma non solo. La grandissima parte delle micro e delle piccole imprese presenta non poche difficoltà nel disporre di risorse economiche e organizzative sufficienti da destinare all'innovazione e alla crescita. Sotto il profilo della sicurezza informatica, le imprese minori sono un bersaglio privilegiato degli attacchi informatici, sia random, sia mirati e per loro le conseguenze negative sono in proporzione ancora maggiori che per le grandi in quanto per loro è sempre più difficoltoso dotarsi di un sistema di protezione per reagire ai danni, economici e d'immagine, causati da una violazione informatica. In conclusione, ci sono diverse ragioni che spingono nella direzione di una risposta in pool ai problemi di sicurezza informatica delle imprese, certamente di quelle più piccole ma anche, con loro, di quelle grandi o medie al vertice di una filiera: consorzio tra imprenditori e contratto di rete. Quest'ultimo è consigliabile soprattutto se non si vuole dar vita a un nuovo soggetto di diritto, ma limitare la collaborazione sul versante Cyber Security alla messa in comune di

[282] V. https://www.enisa.europa.eu/topics/cloud-and-big-data/big-data.

informazioni o alla predisposizione di strumenti di difesa regolati solo sul piano contrattuale attraverso un fondo e un rappresentante comune[283].

[283] G.D. MOSCO, *La collaborazione tra imprese per la sicurezza informatica*, Luiss Law Review, 2017, p. 158 e ss.

CAPITOLO QUARTO

ALLARME CYBERCRIME: UN ALTRO VIRUS VIAGGIA PARALLELO AL COVID-19

SOMMARIO: Introduzione. – 4.1 Analisi del contesto UE. – 4.2. Obiettivi. – 4.3 Metodologia di selezione. – 4.4 Analisi dei dati. – 4.5 Le prospettive future. – 4.6 Considerazioni finali.

Introduzione

L'Europa e l'intera comunità internazionale usciranno trasformate nel post-pandemia a seguito della gestione di una crisi che ha assunto ormai, una dimensione epocale. L'impatto generato dal COVID-19 è ragguardevole a livello sanitario, politico, economico, sociale e psicologico e l'Europa, divisa al primo impatto della pandemia, ha rafforzato in qualche modo, con il sostegno della Banca Centrale Europea e con il varo di Next Generation EU, le possibilità di tenuta del mercato interno. La gestione della Brexit non ha provocato effetti contagio, in un'Europa ormai a diverse velocità, con un peso dominante di Germania e Francia[284]L'utilizzo sempre più diffuso di strumenti informatici e telematici nella vita di tutti i giorni, in questo periodo di emergenza sanitaria, ha prodotto un vertiginoso aumento dei reati commessi in Rete come frodi online, furto d'identità telematica, danneggiamenti ai sistemi telematici, accessi abusivi ai sistemi informatici e molto altro.

L'avvento della tecnologia ha consentito nel tempo interconnessioni a livello globale, permettendo ai soggetti di collegarsi da vari punti nel globo, agendo e comunicando a distanza per cui, gli attori delle dinamiche criminose sono portati a credere che, i comportamenti devianti perpetrati in rete, non producano effetti oltre il contesto virtuale del cyberspace, rafforzando in questo modo una loro convinzione di impunità.

[284] V. G. RACHMAN, "The Perverse Political Effects of Covid-19", Financial Times, 29 dicembre 2020

La principale difficoltà nell'individuare i cyber-criminali è dovuta proprio all'anonimato consentito dalla Rete, alla rapidità di diffusione dei dati e alla facilità con cui riescono a cancellare le proprie tracce.

Nasce da qui quel sentimento di sicurezza relativo al presunto anonimato fornito dal web, legato alla percezione della bassa probabilità che il fatto possa essere scoperto e conseguentemente sanzionato[285]. Il reo non distingue più il confine tra ciò che è lecito e ciò che invece non lo è e percepisce la condotta attuata come meno grave rispetto alla commissione di un reato "tradizionale".

In effetti, le attività poste in essere nel cyberspazio non sono facilmente localizzabili, in quanto a distanza, producono effetti oltre il territorio del singolo Paese e, nel contempo, risulta difficile individuare il luogo e il momento in cui le condotte possono considerarsi realizzate concretamente. Molto spesso diventa problematico individuare con esattezza il responsabile, uno dei limiti del principio di territorialità nel cyberspace. Si tratta, dunque, di comportamenti illeciti atemporali e aterritoriali, caratterizzati dalla transnazionalità. Non di rado succede che il soggetto attivo pone in essere un comportamento deviante in un determinato luogo, ma le conseguenze si esplicano a danno di un sistema informatico, situato in un'area diversa[286].

Le azioni illecite in ambito informatico sembrano produrre oggi nuovi profili di personalità delinquenziali, rendendo inclini soggetti diversi dai criminali tradizionali.

La cybercriminologia ha condotto studi che hanno permesso di delineare alcuni "profili" tipici del cybercriminale: tendenzialmente non-violento; con sviluppata capacità di pianificazione per sfruttare le opportunità dell'informatica; contenimento dell'ansia per l'assenza di contatto con la scena criminis e la vittima oggetto del reato; tendenza ad operare nel tempo in assoluta solitudine; attitudine ad acquisire il know how criminale; minore propensione ad autoconcepirsi quale soggetto criminale. Il criminale informatico ha

[285] A. BALLONI, R. BISI, R. SETTE, *Principi di criminologia applicata*, Cedam, 2015, p.271 e ss.

[286] Sull'argomento G. CASSANO, G. SCORZA, G. VACIAGO (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione e giurisprudenza*, Cedam, Padova, 2012, 551 ss.

elevata preparazione tecnica, cultura superiore, gode della stima dei colleghi, non ha quasi mai precedenti penali e/o disciplinari[287].

È evidente come l'Information Technology possa indurre alcuni soggetti a percepire in maniera alterata il crimine compiuto, facilitando comportamenti criminali che difficilmente attuerebbero al di fuori dal cyberspazio. Basti pensare ai terroristi psicologicamente non inclini ad azioni militari, ai truffatori che non riuscirebbero ad affrontare il cosiddetto face-to-face, oppure donne che non avrebbero il coraggio di prostituirsi per strada, impiegati insoddisfatti che non avrebbero il coraggio di compiere azioni di sabotaggio all'interno della propria azienda, ladri di informazioni che non riuscirebbero ad introdursi in uno spazio fisico per sottrarre informazioni oppure, persone che non riuscirebbero ad insultare o molestare sessualmente nessuno senza avvalersi della mediazione di email o sms nascondendosi dietro un personal computer.

E così anche l'Informatica forense[288] come disciplina si è guadagnata una propria autonomia a causa della forte specializzazione raggiunta e perfezionata nel tempo. Questo perché la scena del crimine è diventata anche digitale e attraverso essa è possibile scoprire la conservazione, identificazione, acquisizione, documentazione, protezione ed interpretazione dei dati presenti su un computer oppure veicolati attraverso la rete, così da poterli valutare come prove utili alla soluzione del "caso"[289].

Nel frattempo, l'emergenza epidemiologica causata dal Covid19 rivela, come si vedrà, una vera e propria pandemia digitale con aziende che sperimentano, durante questo periodo, problemi di sicurezza legati allo smart working[290], mentre il sistema sanitario appare un ulteriore punto critico che caratterizza il momento di incertezza.

---

[287] P. FEDELI, G. RICCI, C. CORTUCCI, *Lineamenti di Criminologia*, Napoli, ESI, 2006, p. 163 e ss.

[288] L'informatica forense è una branca della scienza digitale forense legata alle prove acquisite da computer e altri dispositivi di memorizzazione digitale.

[289] Cfr. G. COSTABILE, *Computer forensic e informatica investigativa alla luce della l. n. 48 del 2008*, in Cyberspazio e diritto, Vol. 11, 2010, n. 3, p. 465 e ss.

[290] Secondo il Ministero del Lavoro e delle Politiche Sociali: "L*o Smart Working (o Lavoro Agile) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e*

Le aziende si preoccupano, giustamente, dei rischi per la sicurezza e dei cambiamenti necessari da affrontare, impegnate nel migliorare la sicurezza dell'accesso da remoto con modifiche veloci alle infrastrutture per gestire gli accessi e tamponare i danni lì dove ormai sono stati generati.

lavoro e, al contempo, favorire la crescita della sua produttività". https://www.lavoro.gov.it/strumenti-e-servizi/smart-working/Pagine/default.aspx

4.1 Analisi del contesto UE

L'11 marzo 2020 l'Organizzazione Mondiale della Sanità[291] ha dichiarato lo stato di pandemia in relazione alla diffusione a livello globale del Covid-19. Come noto, infatti, il virus SARS-CoV-2 a partire dal mese di gennaio 2020 si è diffuso in maniera subdola e repentina dall'Asia all'Europa, così che nel mese di marzo il continente europeo è stato dichiarato dall'OMS epicentro della pandemia. Nelle settimane successive a tale dichiarazione, le misure di lockdown e di distanziamento sociale adottate dai governi nazionali hanno progressivamente portato ad una riduzione dii nuovi contagi. Allo stesso tempo la diffusione del virus è divenuta significativa negli Stati Uniti ed in America Latina. Per arginare la diffusione del virus è arrivato il lockdown, ossia la chiusura prolungata delle attività produttive, commerciali e turistiche insieme al divieto di ogni forma di aggregazione e di importanti limitazioni della libertà di circolazione[292],

La scelta metodologica è quella di comprendere il fenomeno nella sua specificità e complessità e il suo sviluppo nell'ambiente sociale ed economico del contesto europeo.

La criminalità informatica è stata capace di adattarsi velocemente ai radicali cambiamenti nella vita e nelle interazioni tra persone e nello stesso tempo ha saputo cogliere tutte le debolezze che si sono manifestate nel corso di questa pandemia.

Basti riflettere sui numerosi incidenti informatici che hanno avuto un risalto mediatico in questi ultimi due anni, per capire quanto la situazione abbia assunto aspetti particolarmente critici.

[291] A proposito di dichiarazione dell'Organizzazione Mondiale della Sanità si veda WHO DirectorGeneral's opening remarks at the media briefing on COVID-19 - 11 March 2020, in https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid19---11-march-2020.

[292] A proposito di dichiarazione dell'Organizzazione Mondiale della Sanità si veda WHO DirectorGeneral's opening remarks at the media briefing on COVID-19 - 11 March 2020, in https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid19---11-march-2020.

Uno spartiacque tra due epoche con implicazioni e sviluppi sullo scenario globale. Un faro che si accende sull'operato di tutti gli attori internazionali alle prese con sfide importanti, dalla pandemia ancora in corso, al cambiamento climatico fino alla crisi economica. Il primo Paese colpito è stata la Cina, con casi sviluppati nella città di Wuhan[293]. Il virus si è diffuso anche in Italia, pian piano nel resto d'Europa. Successivamente, negli Stati Uniti, e, in misura differente, in tutto il mondo. Infine, ha investito con particolare violenza India e Brasile divenendo una emergenza sanitaria globale.

Il segretario Generale dell'O.N.U. Antonio Guterres[294] ha dichiarato che la pandemia da coronavirus si può definire come "la più grande prova che il mondo deve affrontare dalla seconda guerra mondiale." Il lungo periodo di quarantena istituito dai governanti con la chiusura di molte attività produttive e sospensione di servizi, anche di pubblica utilità è da ritenersi la causa principale di una grave emergenza con ripercussioni sul sistema economico europeo. Ciò potrebbe portare ad una recessione sistemica di portata equiparabile a quella di circa un secolo fa, successivamente alla nota epidemia di "influenza spagnola", con culmine nel 1929 anche se esiste una differenza significativa tra quel momento storico e quello attuale[295]. Tuttavia la pandemia sta facendo precipitare l'Unione Europea nella sua più grande recessione dopo la Seconda Guerra Mondiale. L'epidemia, disgregando il sistema nel suo complesso, ha interessato vari settori: sanitario, economico, sociale, culturale, giuridico e dell'istruzione per cui in questo contesto l'Europa è sembrata smarrirsi, rimanendo arginata e attirando su di sé numerosi giudizi di inadeguatezza[296].

---

293 https://www.rainews.it/articoli/2021/12/Due-anni-fa-le-prime-notizie-su-misteriosi-polmoniti-a-Wuhan-ae3bb3a3-9200-412d-a83e-c9c6c956a19a.html.

294 https://www.europarl.europa.eu/news/it/headlines/eu-affairs/20210622STO06705/guterres-la-pandemia-ha-svelato-la-nostra-comune-fragilita.

295 P. ACCONCI, E. BARONCINI*, Gli effetti dell'emergenza Covid-19 su commercio, investimenti e occupazione*. Una prospettiva italiana (a cura di), Dipartimento di Scienze Giuridiche, Università Bologna, luglio 2020, p.1.

296 Cfr., F. MUNARI, L. CALZOLARI, *Le regole del mercato interno alla prova del COVID19: modeste proposte per provare a guarire dall'ennesimo travaglio di un'Unione incompiuta*, in Eurojus, Speciale 2020; F. ROSSI, Luci ed ombre sull'intervento dell'unione europea a fronte dell'emergenza del Covid-19, in Nomos, 2020, 1 ss.

L’emergenza ha spinto così i cittadini europei a dare maggiore attenzione alle condizioni di sicurezza rispetto ai diritti di libertà. Uno scenario fortemente connotato da un’elevata condizione di incertezza, varietà e multilateralità delle minacce.

Le strutture sanitarie sono state messe a dura prova in tutta Europa, evidenziando l’esigenza di un ripensamento radicale della sanità pubblica e un cambiamento radicalmente di rotta finalizzato a incrementare gli investimenti del settore.

Le vittime sono risultate deboli e indifese e molto spesso del tutto impreparate a fronteggiare le sfide che il mondo cibernetico ha posto ai suoi utilizzatori, tutto ciò non ha fatto altro che favorire il lavoro dei criminali informatici.

Con il lavoro agile sono aumentate le ore trascorse online, spesso attraverso l’utilizzo di dispositivi non sicuri oppure su reti non protette. Tutto ciò ha esposto inevitabilmente, i cittadini europei e le aziende a seri rischi.

È interessante rilevare come, nei periodi di lockdown, si sia riscontrata una diminuzione del numero di reati comuni come rapine, scippi e furti in appartamento a cui ha corrisposto un incremento del numero dei reati legati all’uso degli strumenti elettronici e dell’informatica[297].

Nel contesto europeo anche le pesanti restrizioni imposte[298] per limitare la propagazione della pandemia hanno generato cambiamenti radicali su larga scala ma non hanno purtroppo rallentato l’attività dei criminali informatici. Il cybercrime e le intrusioni mirate hanno anzi registrato una crescita senza precedenti. Il boom degli attacchi è stato implacabile e, per alcune aziende, rovinoso.

Varie critiche sono state mosse nei confronti dell'UE per la sua inerzia e inefficacia percepita almeno in un primo momento, nell'assistere gli Stati membri. L'impatto economico di Covid-19 si è già dimostrato così grave che senza un forte sforzo coordinato i

[297] IL SOLE 24ORE, *I furti e le rapine crollano con il virus ma più reati sul web*, di M. Casadei e M. Finizio, 26 ottobre 2020, https://www.ilsole24ore.com/art/i-furti-e-rapine-crollano-il-virus-ma-piu-reati-web-AD7B5Px.

[298]https://www.penaledp.it/un-anno-di-pandemia-il-diritto-dellemergenza-quadro-normativo-rassegna-di-dottrina-e-giurisprudenza/ .

paesi già indebitati dell'Euro-zona non saranno in grado di superare gli effetti della diffusione del virus[299].

[299] J. HAAS J.C. NEELY, "Central Bank Responses to COVID-19," Economic Synopses, No. 23, 2020.

4.2 Obiettivi

Lo scopo di questo lavoro è di presentare e analizzare il fenomeno nel suo contesto di vita reale, avvalendosi di diverse fonti di analisi, indicate nel paragrafo successivo, con una triangolazione dei dati finalizzata a comparare le informazioni raccolte e valutare il quadro che ne deriva, in termini di causa e di effetto.

Attraverso l'attività di ricerca, s'intende identificare, sintetizzare e valutare alcuni lavori e ricerche pubblicate che risultano rilevanti sull'argomento in questione, allo scopo di affrontare in maniera sistematica il tema "caldo" della Cyber Security.

Un settore che, come abbiamo visto, coinvolge indistintamente governi nazionali, settori militari, servizi di informazione ma anche il sistema economico e il mondo delle imprese nel suo complesso e inevitabilmente, a vario titolo e grado di interesse, ogni cittadino in ogni angolo del mondo.

Vogliamo approfondire così le tendenze della criminalità nel corso della pandemia, a livello europeo, verificando come il cybercrime e la disinformazione ad opera di fakenews online possano risultare tra i fenomeni che maggiormente si sono sviluppati negli ultimi due anni. Sarà importante comprendere il fenomeno nella sua complessità, valutandone l'esistenza in circostanza così rara e straordinaria come l'emergenza sanitaria a livello mondiale.

Sarà interessante comprendere le conseguenze derivanti da campagne di phishing, ransomware, malware o semplici truffe online.

Fenomeni che si sono moltiplicati approfittando della vulnerabilità emotiva delle persone dal momento dell'adozione di misure di contenimento del contagio che imponendo di restare in casa, hanno offerto molto più tempo libero da trascorrere sulla rete Internet.

Nei primi capitoli della tesi è stato sviluppato un inquadramento di carattere teorico analitico che si evolve in questo studio con una disamina di quanto realmente accaduto nel periodo di riferimento.

Poiché s'intende approfondire la tematica attraverso un'analisi critica e comparata viene presentata un'indagine descrittiva articolata e sviluppata attraverso: ricerca delle

fonti, raccolta dei dati, elaborazione ed analisi. Verranno esaminati alcuni report e studi sulla materia, aggiornati al 2021- che riportiamo analiticamente nella metodologia di selezione che segue - che, attraverso analisi statistiche, analizzano l'impatto sull'economia e sul mondo digitale. Il lavoro presenta un approfondimento del contesto della Cybersecurity attraverso le più importanti pubblicazioni in materia. Identifica e analizza le numerose minacce provenienti dal cyberspace oltre a delineare un quadro del rischio cyber per le imprese che rivestono un ruolo di primo piano nel processo di difesa.

4.3 Metodologia di selezione

La raccolta dei dati (data collection) costituisce la prima fase del lavoro. Sono stati presi in considerazione i seguenti studi, aggiornati al 2021, sugli attuali scenari di attacco:

- Indice dell'economia e della società digitali (DESI) 2021[300] riferiti all'anno 2020Clusit[301] (ottobre 2021) Rapporto sulla sicurezza ICT in Italia dell'Associazione Italiana per la Sicurezza Informatica
- Rapporto Europol 2021(IOCTA)[302]
- Relazione 2021 sul panorama delle minacce 2021 dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione («ENISA»). [303]

L'obiettivo degli analisti di cybersecurity è quello di setacciare il web per stanare le vulnerabilità, identificare le minacce in maniera preventiva e analizzare il fenomeno. Aziende, centri studi, pool universitari, agenzie e associazioni specializzate, a livello internazionale, sono impegnati costantemente nella ricerca e nello studio.

Questo tipo di attività viene classificata sotto il nome di Cyber Threat Intelligence e Threat Hunting[304], finalizzata alla ricerca e all'acquisizione di dati, all'elaborazione degli

[300] L'indice di digitalizzazione dell'economia e della società (DESI) è una relazione annuale pubblicata dalla Commissione europea che monitora i progressi compiuti nel settore digitale dagli Stati membri dell'UE. Questa relazione comprende profili nazionali, che aiutano gli Stati membri a individuare settori di intervento prioritari, nei 4 principali ambiti strategici: capitale umano, connettività, integrazione delle tecnologie digitali, servizi pubblici digitali.

[301] CLUSIT, Associazione Italiana per la Sicurezza Informatica, Associazione senza fini di lucro costituita a Milano il 4 luglio 2000. Rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

[302] Il rapporto Europol IOCTA, pubblicato annualmente, offre una valutazione della minaccia rappresentata dalla criminalità organizzata su Internet. È considerato il prodotto strategico di punta di Europol in quanto pone in evidenzia quelle che sono le minacce dinamiche e in continua evoluzione della criminalità informatica.

[303] L'ENISA (Agenzia dell'Unione Europea per la Cybersecurity) pubblica il cyber-threat landscape per il 2021 fornendo un panorama delle minacce informatiche più comuni in Europa, i principali trend di mercato, gli attori più influenti e le tecniche di attacco preferite. È un dossier annuale sul panorama delle minacce sulla cybersecurity nello Spazio Economico Europeo.

stessi e alla produzione di report semestrali o annuali per la cui uscita c'è sempre grande aspettativa e interesse[305].

Questa nuova attenzione posta sulle attività di Cyber Threat Intelligence, denota una presa di consapevolezza da parte del mondo accademico-istituzionale[306]così come di quello aziendale, riguardo all'importanza di prevenire le potenziali minacce nel sistema cyber invece che affrontarne le conseguenze.

A causa del crescente rischio informatico, la cybersecurity si sta rivelando una delle discipline più richieste sul mercato e anche il mondo accademico è sempre più focalizzato su di essa.

[304] Il processo di Cyber Threat Intelligence, è la possibilità di avvalersi di una knowledge base costruita su fonti esterne ed interne al fine di aumentare la conoscenza, efficace nell'affrontare consapevolmente le minacce e diminuire i tempi di identificazione dell'incidente. Fornisce agli analisti ed incident responder una "actionable intelligence", ossia un'informazione analizzata, contestualizzata, tempestiva, accurata e predittiva.

[305] M. CALINGIURI, *Cyber Intelligence. Tra libertà e sicurezza*, Donzelli Editore, 2016, p.11 e ss.

[306] Cyber Threat Intelligence Overview, ENISA Threat Landscape 2021 The ENISA Threat Landscape (ETL) report is the annual report of the European Union Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape. In October 2021, ENISA released the 9th edition of the report that covers a period of reporting starting from April 2020 up to July 2021.

4..4 Analisi dei dati

Partiamo dall'Indice dell'economia e della società digitali (DESI)[307]. Il Digital Economy and Society Index (DESI) riassume gli indicatori sulle prestazioni digitali dell'Europa e tiene traccia dei progressi operati dai Paesi dell'UE. Partendo da questo scenario sarà possibile comprendere e valutare il quadro della sicurezza cyber che si è delineato in questa fase emergenziale. I rapporti DESI 2021, infatti, si basano principalmente sui dati del 2020 e presentano lo stato dell'economia e della società digitali nel primo anno della pandemia.

La Figura n. 1, ci restituisce la fotografia digitale dell'annus horribilis 2020: l'Italia posizionata al 20esimo posto nel ranking complessivo dei 27 Paesi UE (con a capo la Danimarca), di nuovo penultima tra Paesi più popolosi, davanti solo alla Polonia e con rimarchevoli lacune sugli indicatori legati alle competenze digitali.

La Commissione europea pubblica[308]i risultati dell'indice di digitalizzazione dell'economia e della società (Digital Economy and Society Index - DESI), che monitora le prestazioni digitali globali dell'Europa e misura i progressi compiuti dai paesi dell'UE in termini di competitività digitale, ormai dal 2014. Ogni anno, DESI include i profili dei Paesi che supportano gli Stati membri nell'identificare le principali aree digitali, dati essenziali per adottare e supportare le decisioni di carattere politico.

Il 20esimo posto per livello di digitalizzazione dell'economia e della società digitali conferma, in fatto di digitalizzazione, che l'Italia è ancora tra i fanalini di coda dell'Europa.

[307] Il Digital Economy and Society Index (DESI) su base annuale, monitora le prestazioni degli Stati membri in materia di connettività digitale, competenze digitali, attività online e servizi pubblici digitali al fine di valutare lo stato della digitalizzazione di ciascuno Stato membro e identificare le aree che richiedono investimenti e azioni prioritari. DESI comprende 5 dimensioni: Connettività (banda fissa e mobile, prezzi), Capitale umano (uso di Internet, competenze digitali di base e avanzate), Utilizzo dei servizi Internet (utilizzo dei contenuti da parte dei cittadini, comunicazione, transazioni online).

[308] https://ec.europa.eu/commission/presscorner/detail/it/IP_20_1025

Il Rapporto[309]presenta lo stato di fatto nel primo anno della pandemia ed è stato adeguato per riflettere le due principali iniziative di carattere politico destinate a generare un impatto sulla trasformazione digitale nell'Unione nei prossimi anni: il Recovery and Resilience Facility (RRF)[310] e il Digital Decade Compass[311] .

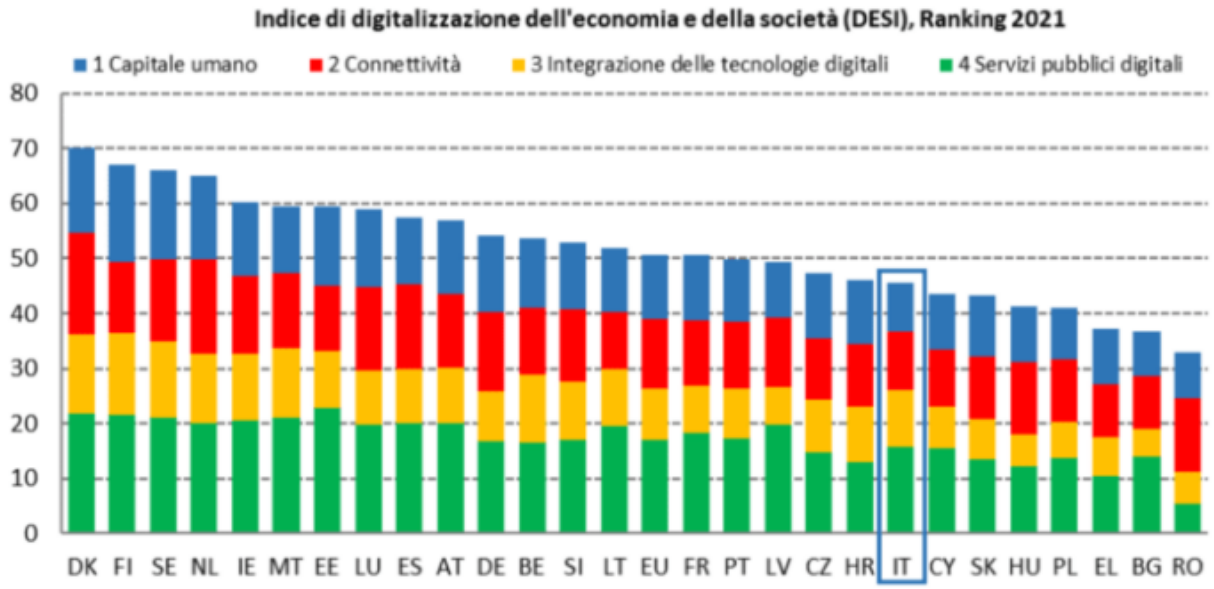


Figura n. 1

[309] Indice dell'economia e della società digitali (DESI) 2021, riferiti all'anno 2020.

[310] RRF, si tratta dello strumento chiave al centro di NextGenerationEU per aiutare l'UE a uscire più forte e più resiliente dalla crisi post pandemia. Consente alla Commissione di raccogliere fondi per aiutare gli Stati membri ad attuare riforme e investimenti in linea con le priorità dell'UE. Mette a disposizione 723,8 miliardi di euro in prestiti (385,8 miliardi di euro) e sovvenzioni (338 miliardi di euro).

[311] Il 9 marzo 2021 la Commissione ha presentato una visione e una serie di prospettive per la trasformazione digitale dell'Europa entro il 2030. Nella Digital Compass la visione e gli obiettivi della trasformazione digitale considerano quattro dimensioni: competenze digitali/capitale umano, infrastrutture digitali, trasformazione digitale delle imprese, digitalizzazione dei servizi pubblici.

Clusit, Rapporto 2021 sulla sicurezza ICT in Italia

I dati relativi alla nuova edizione del Rapporto Clusit 2021[312], Associazione Italiana per la Sicurezza Informatica, evidenziano, per i primi sei mesi del 2021, un aggravamento della situazione sul fronte della sicurezza cyber.

Il 25% degli attacchi mappati nel primo semestre è stato diretto verso l'Europa. Gli attacchi verso realtà basate in Europa, infatti, aumentano sensibilmente dal 15% al 25%.

Il dato risulta piuttosto interessante perché la classificazione delle vittime per nazione di appartenenza viene rappresentata su base continentale. Nel 1 semestre 2021 rimangono sostanzialmente invariate le vittime di area americana (dal 45% passano al 46%) mentre rimangono percentualmente quasi invariati quelli rilevati contro organizzazioni asiatiche.

Diminuiscono, invece, gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (riferiti alla categoria "Several / Multiple"), che dal 25% del 1 semestre 2020 passano al 16% (Figura n.2).

[312] Clusit (ottobre 2021) Rapporto sulla sicurezza ICT in Italia dell'Associazione Italiana per la Sicurezza informatica.

Distribuzione generale delle vittime per area geografica (1H 2021)

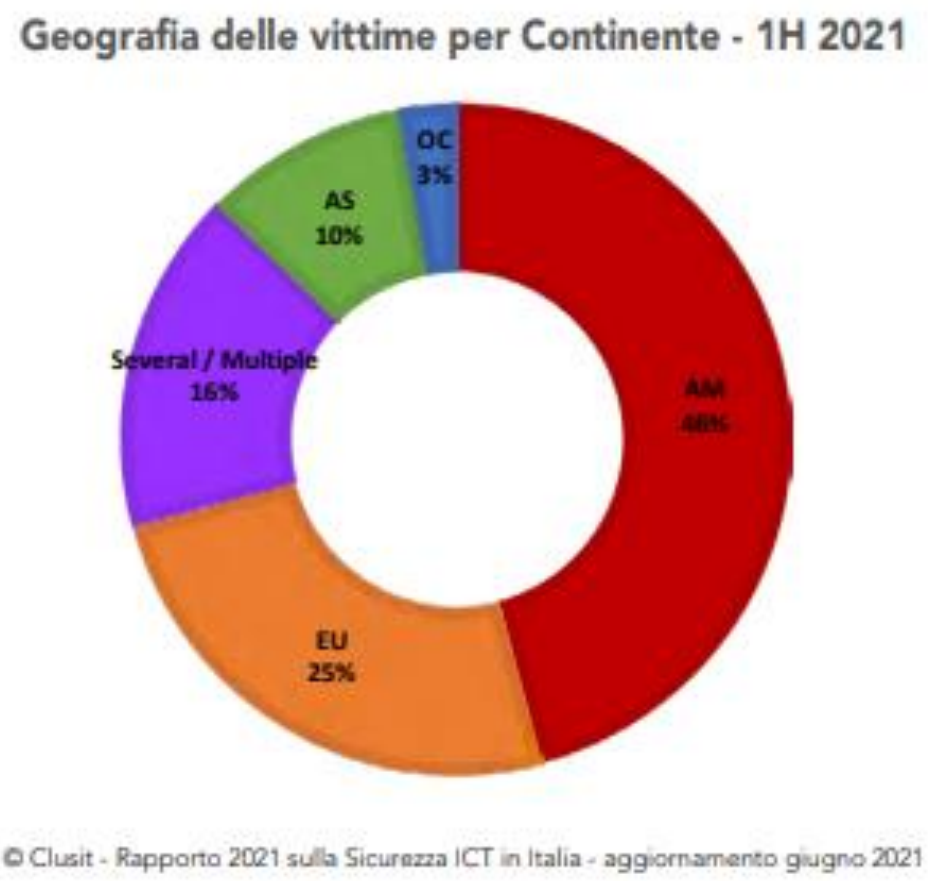


Figura n.2

È possibile quindi affermare che pur dovendo ritenere il 2020 come l'anno peggiore di sempre in termini di evoluzione delle minacce cyber e dei relativi impatti[313] evidenziando un trend persistente di crescita degli attacchi, della loro gravità nonchè dei danni conseguenti, tale tendenza negativa si conferma ampiamente anche nel primo semestre 2021 stando ai dati che emergono con chiarezza dalla ricerca.

[313] Clusit (ottobre 2021) Rapporto sulla sicurezza ICT in Italia dell'Associazione Italiana per la Sicurezza Informatica, p.11

Le perdite derivanti da questa situazione di Far West digitale sono ingenti, stimate in 1 trilione di dollari per il 2020 e 6 trilioni per il 2021. Dati che dovrebbero far riflettere seriamente, dinamiche pericolose che rappresentano un'emergenza globale e incidono ormai per una percentuale significativa del GDP[314] mondiale.

Il report si è avvalso anche in questa edizione dei dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB[315], che nella prima metà del 2021 (dal 1° gennaio al 31 agosto), ha registrato 36 Milioni di eventi malevoli, in forte aumento rispetto allo stesso periodo dell'anno precedente (+180%).

Osservando la situazione da un punto di vista quantitativo, confrontando i numeri del primo semestre 2018 con quelli del primo semestre 2021, risulta che la crescita degli attacchi gravi sia stata del 30% (ossia da 745 a 1.053).

Il Rapporto CLUSIT 2021[316] aggiornato ad ottobre, ha proposto un quadro dettagliato degli incidenti di sicurezza più significativi avvenuti a livello globale l'anno prima e nei primi 6 mesi dell'anno del 2021, confrontandoli però significativamente con i dati raccolti negli ultimi 3 anni (FIGURA N.3).

Lo studio si è basato su un campione che al 30 giugno 2021 era costituito da 13.014 attacchi noti di particolare gravità. Si riferiscono a quelli che hanno causato un impatto significativo in termini di perdite economiche, danni alla reputazione, diffusione di dati sensibili o che comunque prefigurano degli scenari molto preoccupanti, avvenuti a livello globale dal primo gennaio 2011.

1.874 nel 2020 e 1.053 nel primo semestre 2021 e complessivamente 6.148 attacchi rilevati tra gennaio 2018 e giugno 2020 (dunque, quasi la metà del totale).

---

[314] GDP, un indicatore statistico macroeconomico che esprime il valore aggregato di beni e servizi finali prodotti nel territorio di un determinato Paese a prezzi di mercato.

[315] Security Operations Center (SOC), l'analisi inserita all'interno del Rapporto Clusit 2021, dell'Associazione Italiana per la Sicurezza Informatica sulla sicurezza ICT. Si basa sugli attacchi informatici transitati sull'infrastruttura di Fastweb.

[316] Clusit (ottobre 2021) Rapporto sulla sicurezza ICT in Italia dell'Associazione Italiana per la Sicurezza Informatica.

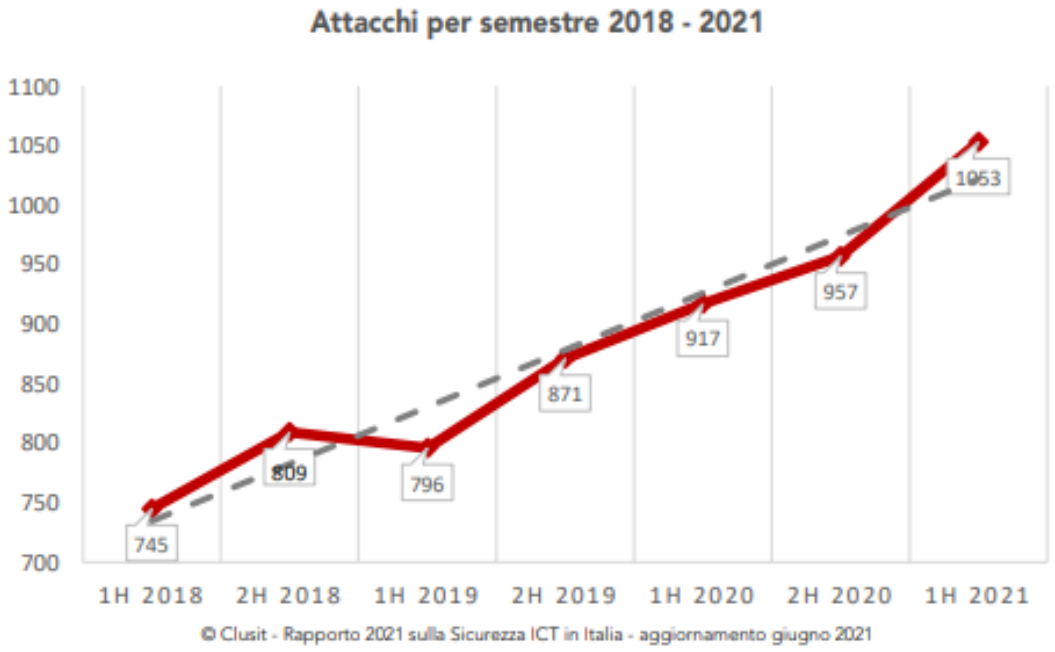


Figura n.3

Dal punto di vista numerico, dei 13.014 attacchi gravi di pubblico dominio che costituiscono il database di incidenti degli ultimi 10 anni, nel 2020 ne abbiamo raccolti e analizzati 1.874, contro i 1.667 del 2019 (+12%), con una media complessiva di 107 attaccchi gravi al mese (erano 39 nel 2011, 130 nel 2018, e sono 176 nel primo semestre 2021). Il picco massimo è stato registrato ad aprile 2021 (204 attacchi). Nella Figura n. 4 la distribuzione mensile degli attacchi registrati nel primo semestre 2021.

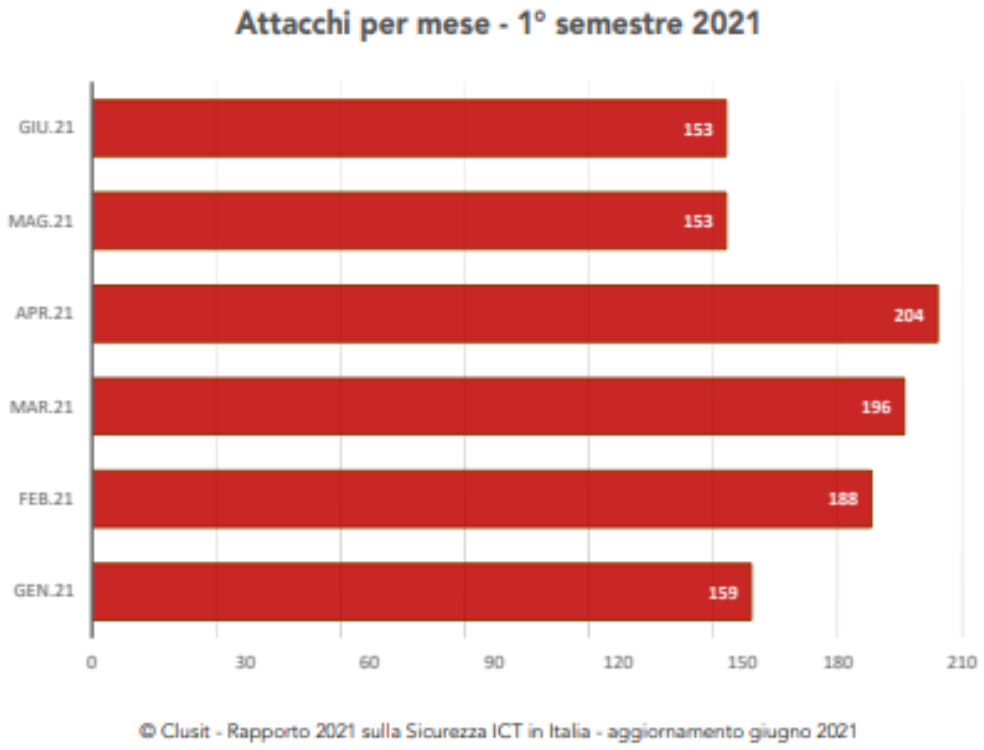


Figura n.4

Rispetto al secondo semestre 2020, il numero di attacchi gravi di dominio pubblico (FIGURA N.5) raccolti e riferiti al primo semestre 2021 appare in crescita del 10% (957 contro 1.053).

In termini assoluti nel 2020 le categorie "Cybercrime", "Cyber Espionage" e"Information Warfare" fanno registrare il numero di attacchi più elevato degli ultimi dieci anni, una tendenza che trova conferma anche nel primo semestre 2021.

Rispetto al secondo semestre 2020 le attività riferibili ad attacchi della categoria "Hacktivism" diminuiscono ancora sensibilmente in termini percentuali (-66,7%), mentre nel primo semestre 2021 dal campione emerge che sono in crescita sia gli attacchi gravi compiuti per finalità di "Cybercrime" (+21,1%) sia quelli riferibili a "Information Warfare" (+18,2%).

Diminuiscono gli attacchi classificati come attività di "Cyber Espionage[317]" (-36,7%) dopo il picco straordinario del 2020, dovuti soprattutto ad attività di spionaggio per lo sviluppo di vaccini e cure per il Covid-19).

Distribuzione degli attaccanti per tipologia (2018 – 1H 2021)

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2H 2020	1H 2021	1H 2021 su 2H 2020	Trend 2021
Cybercrime	1.229	1.381	1.518	764	925	21.1%	↑
Espionage-Sabotage	203	203	264	150	95	-36.7%	↗
Hacktivism	64	48	48	21	7	-66.7%	↓
Information Warfare	58	35	44	22	26	18.2%	↑
Espionage-Sabotage + Inf. Warfare	261	238	308	172	121	-29.65%	↗

Figura n.5

[317] Il cyber espionage è una pratica in continua crescita usata per rubare know-how e informazioni riservate alle aziende pubbliche e private

Nel 2021 il Clusit ha introdotto una tassonomia delle vittime derivata da standard internazionali, articolata su 20 macro-categorie.

VITTIME PER CATEGORIA	2018	2019	2020	2H 2020	1H 2021	1H 21 su 2H 20	TREND
Government, Military, Law Enforcement	220	233	224	120	167	39.2%	↑
Healthcare	161	186	210	117	139	18.8%	↑
Multiple Targets	326	406	401	158	121	-23.4%	↓
Information Communication Technology	191	233	269	149	113	-24.2%	↓
Education	106	140	174	103	100	-2.9%	↗
Financial, Insurance	162	107	122	66	60	-9.1%	↗
Professional, Scientific, Technical	18	19	59	27	50	85.2%	↑
Wholesale, Retail	33	45	54	31	50	61.3%	↑
Transportation, Storage	35	20	44	23	48	108.7%	↑
Manufacturing	32	32	61	32	47	46.9%	↑
News, Multimedia	70	69	43	23	38	65.2%	↑
Organizations	40	35	46	29	30	3.4%	↗
Arts, Entertainment	68	55	40	19	26	36.8%	↑
Energy, Utilities	24	25	39	13	19	46.2%	↑
Hospitability	44	27	22	12	17	41.7%	↑
Other Services	9	14	21	13	13	0.0%	-
Telecommunications	13	19	32	16	9	-43.8%	↓
Construction	1	2	7	4	3	-25.0%	↗
Agriculture, Forestry, Fishing	0	0	5	2	3	50.0%	↑
hMining, Quarrying	1	0	1	0	0	0.0%	-
TOTALE	1.554	1.667	1.874	957	1.053		

[9] ISIC (International Standard Industrial Classification of All Economic Activities) delle Nazioni Unite e NACE della Commissione Europea (Nomenclature statistique des activités économiques dans la Communauté Européenne)

Figura n.6

La crescita maggiore (FIGURA N.6) per quanto concerne gli attacchi gravi si osserva verso le categorie "Transportation / Storage" (+108,7%), "Professional, Scientific, Technical" (+85,2%) e News & Multimedia" (+65,2%), seguite da "Wholesale / Retail" (+61,3%) e"Manufacturing" (+46,9%). Aumentano anche gli attacchi verso le categorie "Energy / Utilities" (+46,2%), "Government" (+39,2%), "Arts / Entertainment" (+36,8%) e "Healthcare" (+18,8%).

Diminuiscono in modo sensibile gli attacchi verso le categorie "Telecommunications" (-43,8%) ed "Information Communication Technology" (-24,2%), ed in misura minore verso "Financial / Insurance" (-9,1%) ed "Education" (-2,9%).

Il calo degli attacchi verso la categoria "Multiple Targets" dove confluiscono una parte degli attacchi verso vittime appartenenti a tutte le altre[318] rappresenta un cambio di strategia da parte degli attaccanti ma anche un preoccupante campanello di allarme: si assiste infatti all'aumento di attacchi gravi mirati verso singoli bersagli, in particolare di tipo ransomware con l'aggravante della "double extortion", cioè della minaccia di diffondere i dati sottratti qualora le vittime non paghino il riscatto.

Nel primo semestre 2021 erano il 12% del totale degli attacchi, in diminuzione del 23,4% rispetto al 2020. Molto significativa risulta la distribuzione delle tecniche di attacco (2018 – 1H 2021) articolata su 8 macro-categorie nella rappresentazione che segue (FIGURE N.7 E N.8).

[318] Clusit (ottobre 2021) Rapporto sulla sicurezza ICT in Italia dell'Associazione Italiana per la Sicurezza Informatica, p.24

Tecniche di attacco	2018	2019	2020	2H 2020	1H 2021	1H 2021 su 2H 2020	TREND
Malware	601	737	776	411	454	10.5%	↑
Unknown	429	309	368	202	230	13.9%	↑
Vulnerabilities	143	158	198	116	164	41.4%	↑
Phishing, Social Engineering	170	291	299	108	94	-13.0%	↘
Multiple Techniques	64	57	85	43	48	11.6%	↑
Identity Theft, Account Cracking	67	71	90	44	31	-29.5%	↓
Web Attack	43	21	17	12	20	66.7%	↑
Denial Of Service	37	23	34	21	12	-42.9%	↓
TOTALE	1.554	1.667	1.874	957	1.053		

Figura n.7

Nel 1H 2021 la categoria con numeri assoluti maggiori è “Malware” (+10,5%), che costituisce il 43% del totale. Le tecniche sconosciute sotto la categoria “Unknown” tornano al secondo posto, con un aumento del 13,9% rispetto al 2H 2020. Superano così la categoria “Vulnerabilità note” che fa registrare un preoccupante +41,4% e“Phishing / Social Engineering” (in calo, -13%), mentre “Tecniche Multiple” sale del +11.6%. Per passare poi agli attacchi gravi, quelli con finalità di “Denial of Service” diminuiscono del 42,9%, così come quelli realizzati tramite “Identity Theft / Account Hacking” che si attesta al 29,5%.

Panoramica dei cyber attacchi più significativi del 2018-2020 e del primo semestre 2021

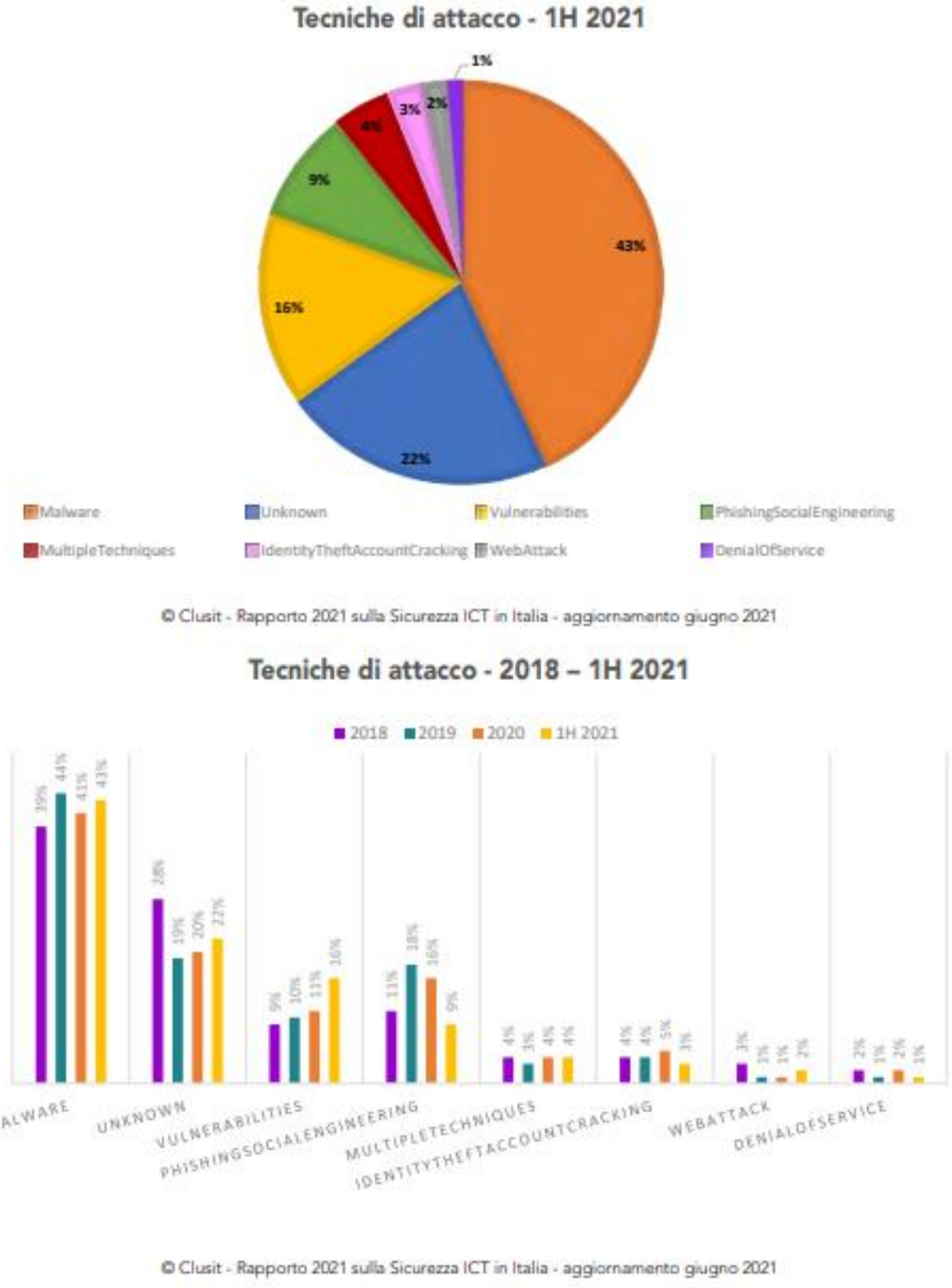


Figura n.8

Per quanto riguarda la severity (FIGURA N.9), nel 2020 gli attacchi cosiddetti con impatto “Critico” costituivano il 13% del totale, quelli di livello “Alto” il 36%, quelli di livello “Medio” il 32% e infine quelli che raggiungevano il livello “Basso” erano il 19%.

In totale, gli attacchi gravi con effetti importanti (High) o addirittura devastanti (Critical) nel 2020 hanno raggiunto il 49% del campione. Nel primo semestre 2021 la situazione risulta molto diversa e sicuramente preoccupante. Gli attacchi gravi (High) sono il 49%, quelli devastanti (Critical) rappresentano il 25%, quelli di impatto significativo (Medium) il 22%, e, infine, quelli con impatto basso raggiungono una percentuale del 4%. In questo caso gli attacchi con impatto Critical e High nel totale sono il 74%.

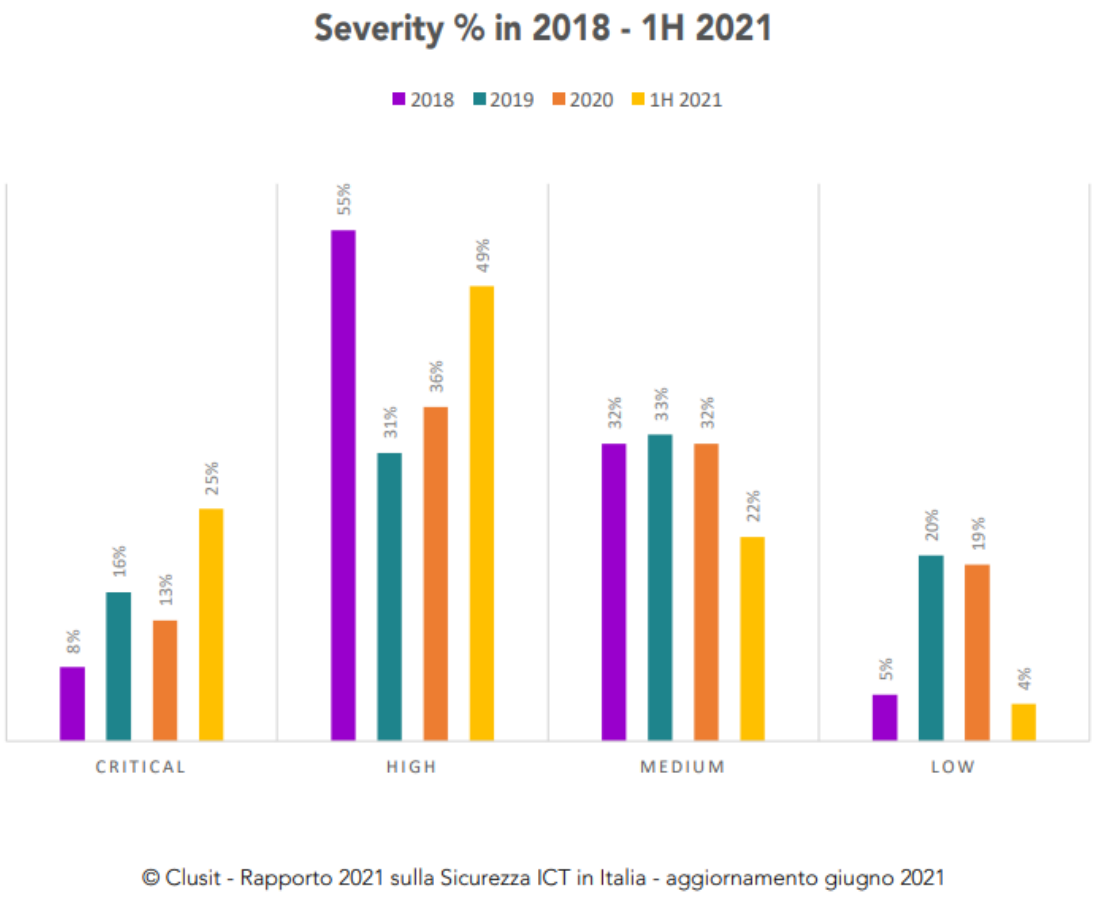


Figura n.9

Rapporto Europol 2021(IOCTA)

Anche nel Rapporto Europol 2021 (IOCTA)[319], l'impatto della pandemia di COVID-19 emerge con forza evidenziando come la digitalizzazione sia stata accelerata dalla emergenza sanitaria influenzando in maniera significativa la diffusione delle minacce informatiche.

L'IOCTA è il prodotto strategico di punta di Europol che fornisce una valutazione basata sull'applicazione della legge delle minacce in evoluzione e degli sviluppi nel settore della criminalità informatica. Dall'analisi emerge che i programmi ransomware hanno consentito a gruppi di criminali di attaccare aziende e istituzioni pubbliche minacciandole con metodi di estorsione multilivello come gli attacchi DDoS. Il malware mobile si è evoluto con l'elusione di ulteriori misure di sicurezza come l'autenticazione a due fattori. Inoltre, è stato evidenziato come lo shopping online abbia portato a un forte aumento delle frodi online. I criminali infine continuano a fare largo uso di servizi legittimi come VPN, servizi di comunicazione crittografati e criptovalute.

In particolare, vengono descritte le attività messe in atto dalle reti criminali nell'Ue e il modo in cui le costituiscono una minaccia per la società, l'economia e le istituzioni: «la criminalità organizzata non ha mai rappresentato una minaccia così elevata per l'Unione europea e i suoi cittadini come oggi».

Il momento pandemico e le ricadute sociali ed economiche[320] che sembrano inevitabili stanno creando un ambiente estremamente favorevole alla estensione della criminalità organizzata in ambito europeo[321]. Quanto all'impatto della pandemia sulla cibercriminalità[322] era inevitabile che i criminali sapessero rapidamente sfruttare i

[319] Internet Organised Crime Threat Assessment Report (IOCTA) 2021, con la valutazione sulle minacce della criminalità informatica, p.8.

[320] Report (IOCTA) 2021, op.cit. p.11.

[321] https://www.antiriciclaggiocompliance.it/rapporto-socta-2021-e-la-concretezza-della-minaccia-della-criminalita-organizzata-in-europa/.

[322] Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità nell'UE (SOCTA), relazione 2021, Europol.

cambiamenti dettati dal telelavoro e dall'aumento dell'utilizzo dei servizi online al fine di adattare le loro attività illegali al contesto di crisi.

La "Relazione Annuale" (relativa al 2020), della Direzione Centrale per i Servizi Antidroga323 presenta un quadro riassuntivo delle attività eseguite e dei risultati ottenuti dal Paese nella lotta contro il traffico illecito delle sostanze stupefacenti. Su questo anche l'Agenzia Europea per la Droga" ("OEDT"[324]) ed Europol hanno indicato, nei propri report, come in Europa sia aumentato notevolmente il numero di consumatori che acquista sostanze stupefacenti online.

A proposito di narcotraffico sul web, al fine di comprendere i cambiamenti, la portata e la natura dei traffici di droga all'interno dei mercati on line ed in particolare nel Darknet[325], durante la pandemia di Covid 19, sono stati organizzati gruppi di ricerca in tutta la Comunità Europea per raccogliere ed elaborare informazioni utili. In particolare, la regione Veneto risulta un punto strategico per i traffici con il vicino Oriente. Infaţti, i porti di Venezia e Chioggia sembrano essere collegamenti persistenti con quelli del Medio Oriente, in particolare con Istanbul.

In Italia, il dossier Viminale[326] che viene pubblicato ogni anno in occasione della tradizionale riunione del Comitato nazionale per l'ordine e la sicurezza pubblica nel mese

323 La Direzione Centrale per I Servizi Antidroga **è un** organismo interforze **istituito nell'ambito del** Dipartimento della Pubblica Sicurezza ed opera alle dipendenze del Capo della Polizia – Direttore Generale della Pubblica Sicurezza, per l'attuazione delle direttive emanate dal Ministro dell'Interno per la prevenzione e repressione del traffico illecito di sostanze stupefacenti e psicotrope.

324 L'Osservatorio europeo delle droghe e delle tossicodipendenze è un'agenzia dell'Unione europea. È stata fondata nel 1993 e ha sede a Lisbona, in Portogallo. È il centro di informazione sulle droghe e sulle tossicodipendenze dell'Unione europea.

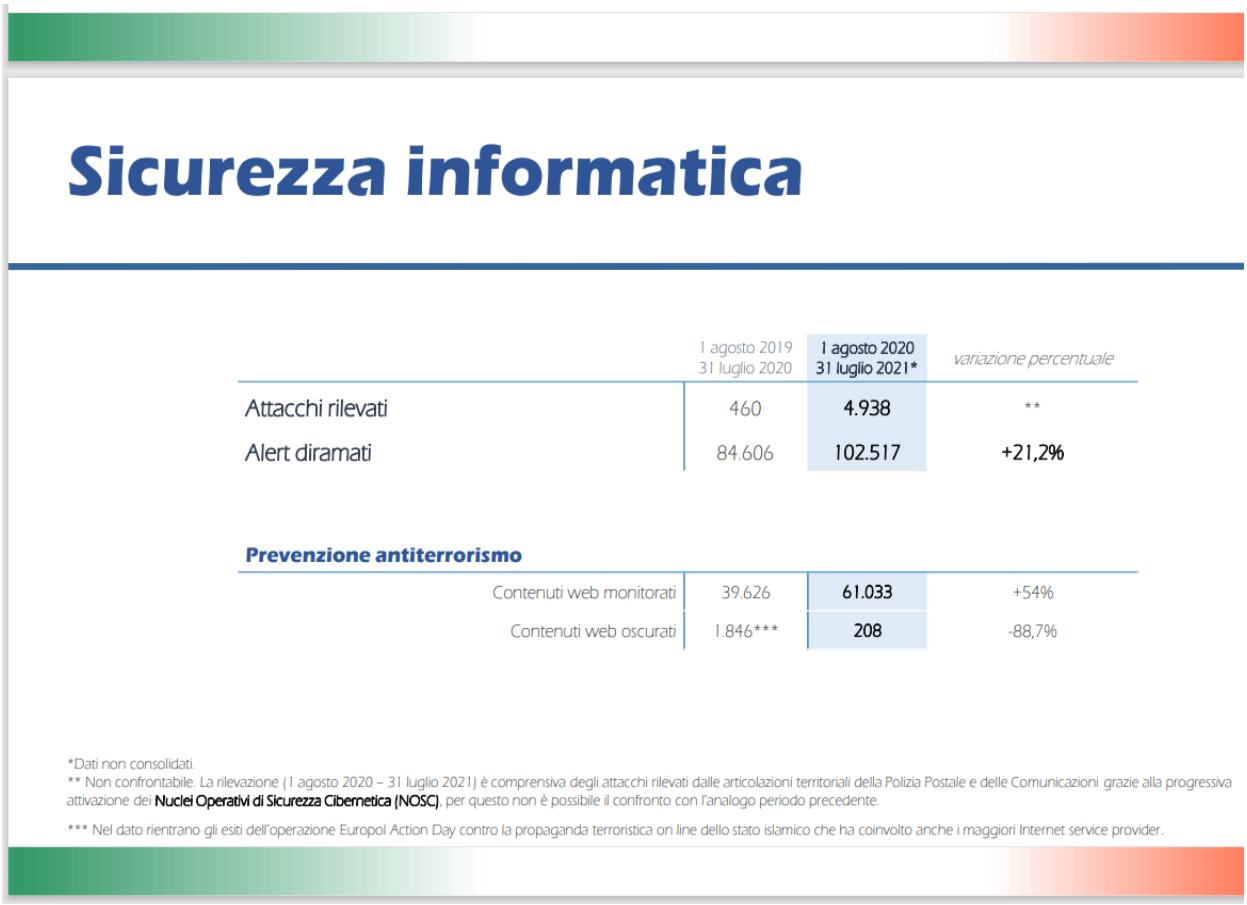
325 "Relazione Annuale" (relativa al 2020), della Direzione Centrale per i Servizi Antidroga, Ministero dell'Interno, Dipartimento della pubblica sicurezza, direzione centrale dei servizi antidroga, 2021, antidroga.interno.gov.it

326 Il dossier Viminale (1 AGOSTO 2020 - 31 LUGLIO 2021*). Un anno di attività del Ministero dell'Interno,* interno.gov.it offre un quadro riassuntivo delle attività e delle iniziative di tutte le componenti del ministero dell'Interno, affrontando il tema della sicurezza – come safety e security – anche attraverso il confronto con il periodo precedente.

di agosto, ha offerto un quadro riassuntivo delle attività affrontando il tema della sicurezza, intesa come safety e securit, attraverso un confronto con il periodo precedente.

Nella tabella di seguito riportata (FIGURA N. 10) è possibile osservare l'aumento rilevante degli attacchi rilevati e l'attività di prevenzione antiterrorismo messa in atto.

I dati si riferiscono al periodo 1 agosto 2020 – 31 luglio 2021



Sicurezza informatica

	1 agosto 2019 31 luglio 2020	1 agosto 2020 31 luglio 2021*	variazione percentuale
Attacchi rilevati	460	4.938	**
Alert diramati	84.606	102.517	+21,2%
Prevenzione antiterrorismo			
Contenuti web monitorati	39.626	61.033	+54%
Contenuti web oscurati	1.846***	208	-88,7%

*Dati non consolidati.
** Non confrontabile. La rilevazione (1 agosto 2020 – 31 luglio 2021) è comprensiva degli attacchi rilevati dalle articolazioni territoriali della Polizia Postale e delle Comunicazioni grazie alla progressiva attivazione dei **Nuclei Operativi di Sicurezza Cibernetica (NOSC)**, per questo non è possibile il confronto con l'analogo periodo precedente.
*** Nel dato rientrano gli esiti dell'operazione Europol Action Day contro la propaganda terroristica on line dello stato islamico che ha coinvolto anche i maggiori Internet service provider.

Figura n. 10

La tabella che segue (Figura n.11), invece, mette in evidenza la crescita dei reati informatici dal 2019 al 2020 rilevata dal Dipartimento della Pubblica sicurezza Direzione centrale della polizia criminale[327].

Figura n.11

Il Rapporto ENISA Threat Landscape (ETL)

Il rapporto ENISA Threat Landscape (ETL) è il rapporto annuale dell'Agenzia dell'Unione europea per la sicurezza informatica, ENISA, sullo stato del panorama delle minacce alla sicurezza informatica. Nel mese di ottobre 2021 l'ENISA ha pubblicato la

[327] La Direzione centrale della polizia criminale è un'articolazione del dipartimento della Pubblica Sicurezza, alla quale è preposto il vice direttore generale della Pubblica Sicurezza, direttore centrale della Polizia Criminale. Quest'ultimo assicura i collegamenti tra la DIA e gli altri uffici, reparti e strutture delle Forze di polizia, nonché il raccordo con le attività della direzione centrale dei Servizi Antidroga.

nona edizione del rapporto che racchiude il periodo che va da aprile 2020 fino a luglio 2021.

Il rapporto identifica le principali minacce e tendenze osservate, gli attori e le tecniche di attacco.

Le 9 minacce principali evidenziate sono: ransomware, malware, criptojacking, minacce legate alla posta elettronica, minacce contro i dati, minacce alla disponibilità e all'integrità, disinformazione, minacce non dannose, attacchi alla catena di approvvigionamento.

In particolare anche in questo caso come abbiamo visto nei report precedenti il ransomware viene valutato come la principale minaccia per il 2020-2021 mentre i criminali informatici sono sempre più motivati dalla monetizzazione delle loro attività.

La criptovaluta rimane il metodo di pagamento più comune per i protagonisti di queste minacce. Il volume delle infezioni da cryptojacking[328] ha raggiunto un livello record nel primo trimestre del 2021, rispetto agli ultimi anni. Il COVID-19 è ancora il sistema di esca prevalente nelle campagne di attacchi via e-mail con una impennata delle violazioni dei dati relative al settore sanitario. Le tradizionali campagne DDoS (Distributed Denial of Service) nel 2021 sono più mirate, più persistenti e sempre più multivettoriali. L' IoT (Internet of Things) in combinazione con le reti mobili sta provocando una nuova ondata di attacchi DDoS.

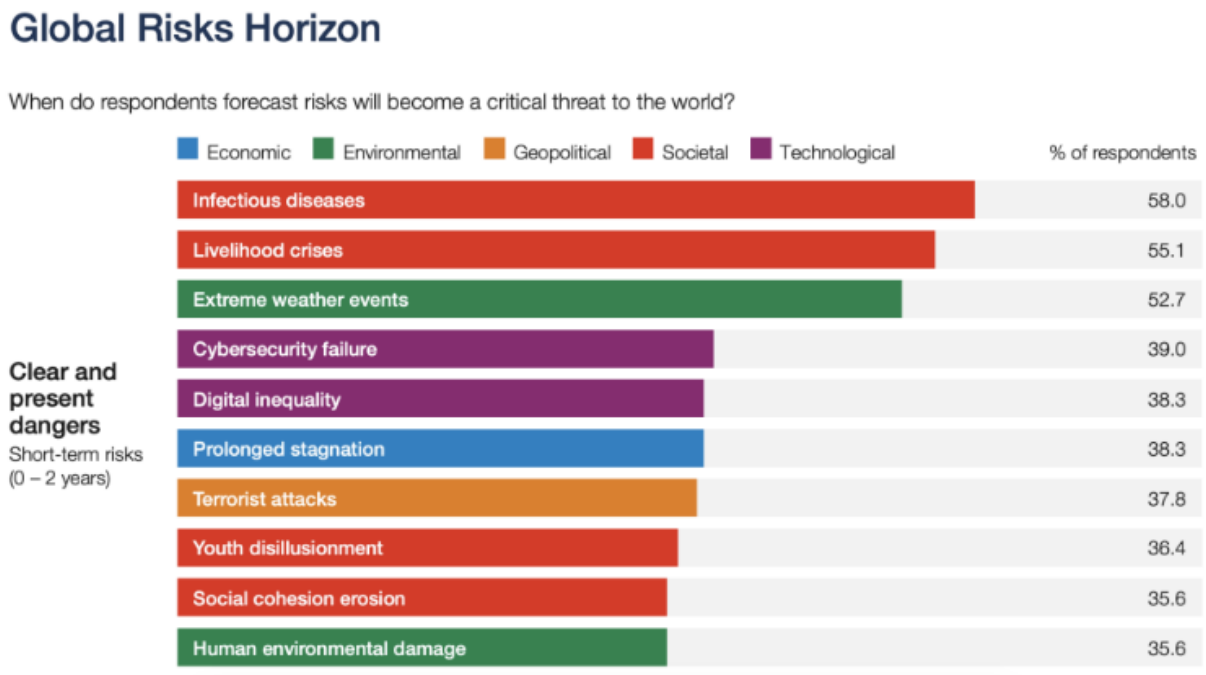
Nel 2020 e nel 2021 si osserva anche un picco di incidenti non dolosi, poiché la pandemia di COVID-19 è diventata un moltiplicatore di errori umani e configurazioni errate del sistema, fino al punto che la maggior parte delle violazioni nel 2020 sono state causate da errori.

[328] Il cryptojacking o cryptomining nascosto è un crimine informatico in cui si utilizza segretamente la potenza di calcolo di una vittima per generare criptovaluta. La vittima installa inconsapevolmente un programma con script dannosi che consentono al criminale informatico di accedere al proprio computer o ad altri dispositivi connessi a Internet. La criptovaluta è denaro digitale o virtuale, che assume la forma di gettoni o "monete". La più nota è Bitcoin, ma esistono circa 3.000 altre forme di criptovaluta, la maggior parte rimane virtuale.

4.5 Le prospettive future

Gli attacchi informatici rappresentano il principale pericolo globale legato alla tecnologia. Lo rileva la sedicesima edizione del Global Risks Report 2021 del World Economic Forum (WEF[329]), che ha analizzato i rischi futuri di carattere economico, ambientale, geopolitico, sociale e tecnologico nei prossimi dieci anni.

In base al report (FIGURA N.12) le infrastrutture e la cybersecurity di aziende, istituzioni governative e famiglie sono violate da crimini informatici sempre più sofisticati, con conseguenti perdite finanziarie, inevitabili tensioni geopolitiche e forte instabilità sociale.



Fonte: Global Risks Report 2021

Figura n.12

[329] Il Forum economico mondiale (in inglese: World Economic Forum, conosciuto anche come Forum di Davos) è una fondazione senza fini di lucro, con sede a Cologny, in Svizzera, nata nel 1971 per iniziativa dell'economista ed accademico Klaus Schwab.

Tra i rischi più plausibili dei prossimi dieci anni ci sono i cambiamenti climatici e i danni ambientali causati dall'uomo, ma per quanto riguarda la tecnologia, il report afferma che il "fallimento della sicurezza informatica" rappresenta il principale rischio tecnologico, con il 39% degli intervistati che ha ritenuto questo un "pericolo evidente e presente" per il mondo nei prossimi due anni.

Secondo il rapporto, gli attacchi informatici dovrebbero aumentare costantemente, insieme alla diffusione di disinformazione, alle fake news e alla manipolazione elettorale e i criminal hacker saranno impegnati in attacchi informatici pericolosi e sempre più sofisticati. La legislazione dell'UE in questo ambito, e in particolare la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) e la direttiva sulle infrastrutture critiche europee (direttiva ECI)[330], ha offerto una valida base per reagire ai recenti incidenti.

Del resto, uno dei padri fondatori dell'Unione europea, l'intellettuale francese Jean Monnet[331] nelle sue Mémoires[332] afferma che: «L'Europa sarà forgiata dalle sue crisi e sarà la somma delle soluzioni trovate per risolvere tali crisi». Ciò sta a significare che il progetto europeo non può essere rappresentato solo da istituzioni distanti ma dalla volontà di trovare soluzioni comuni a problemi comuni. Mai come oggi la frase pronunciata da Jean Monnet nell'agosto del 1954 risuona come una triste verità.

Nel contempo, però, la maggiore incidenza e intensità delle minacce dimostra che l'attuale quadro legislativo non è adeguato allo scopo. Da una valutazione dello stato di attuazione della direttiva NIS è emerso che il suo ambito di applicazione non rispecchia il livello attuale di digitalizzazione e interconnessione, né l'interdipendenza di settori economici e sociali fondamentali.

[330] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[331] Politico ed economista francese (Cognac 1888 - Houjarray 1979) Jean Monnet è considerato uno dei padri dell'Europa, anzi il padre dell'Europa comunitaria, poiché si deve alla sua ispirazione il Piano Schuman del 9 maggio 1950 (il 9 maggio è poi diventata la data di compleanno dalla UE).

[332] J. MONNET, *Mémoires*, Paris, Fayard, 1976.

Alcuni enti pubblici e privati, appartenenti a settori essenziali inoltre, non sono subordinati alla direttiva o non sono tenuti a rispettare gli obblighi in fatto di cibersicurezza non armonizzata e di segnalazione di incidenti. Nel dicembre 2020 la Commissione ha pertanto proposto due importanti atti legislativi: una direttiva sulla resilienza dei soggetti critici (CER)[333] e una direttiva rivista relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS rivista)[334]

Tutte e due le direttive hanno un ambito di applicazione molto ampio, che copre gli stessi dieci settori essenziali quali trasporti, energia, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, PA e spazio. In questi settori la direttiva CER avanza misure per istituire un quadro di resilienza fisica con norme minime che consentano la flessibilità necessaria.

La proposta di direttiva NIS rivista introdurrebbe nuovi strumenti per la gestione e la divulgazione delle vulnerabilità, nonché per una maggiore risposta agli incidenti e nella gestione delle crisi, razionalizzando anche gli obblighi di segnalazione degli incidenti dettando disposizioni più precise sulla procedura, sul contenuto e sulla tempistica della segnalazione. La relazione della proposta per la cd. "NIS 2" [335]riconosce, da una parte, che la direttiva NIS ha contribuito a migliorare le capacità di cybersecurity a livello nazionale, richiedendo agli Stati membri di adottare strategie nazionali e di nominare ove necessario le autorità competenti NIS e ad aumentare la cooperazione a livello dell'Unione, istituendo vari forum volti a facilitare lo scambio di informazioni strategiche e operative. Dall'altra, la valutazione del funzionamento della direttiva ha evidenziato diversi e significativi problemi.

[333] Direttiva CER, Resilience of Critical Entities, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. 14262/20 + ADD 1.

[334] Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

[335] COMMISSIONE EUROPEA, Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) COM (2020) 823 final.

4.6 Considerazioni finali

Dallo svolgimento di questo lavoro si comprende come, nonostante i vari sforzi anche in campo internazionale, ci siano diversi livelli di idoneità a combattere tali crimini tra i diversi Paesi. La speranza è che le più serie implicazioni sanitarie possano lasciare spazio a nuovi e migliori scenari economici, politici e sociali generati dalla pandemia.

Con la diffusione del virus da Covid-19 si è registrato un incremento dell'attività di cybercrime in tutto il mondo, con una particolare diffusione di attacchi ransomware.

Il ricorso al lavoro agile, alla DAD (didattica a distanza), alla telemedicina e al commercio elettronico ha accresciuto la quantità dei dati personali in rete. Secondo gli esperti gli ultimi due anni sono stati difficili per le infrastrutture strategiche, per la ricerca e le istituzioni governative. Gli attacchi subiti, per natura, gravità e dimensione vanno oltre i confini dell'ICT e della stessa Cyber Security con impatti sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica.

Il ransomware non dà segni di indebolimento mentre si osserva un cambiamento delle tattiche di assalto. Gli attacchi provengono da organizzazioni di dimensioni sempre più elevate e i professionisti dell'IT si trovano a dover adottare una strategia proattiva per affrontare queste nuove tendenze e le sfide che si prospettano all'orizzonte.

L'aspetto più preoccupante è rappresentato dall'incremento dell'attività dei ransomware con richiesta di riscatto. Infatti, è stata osservata una crescita dell'attività di questo malware di circa il 350% rispetto allo stesso periodo dell'anno precedente[336]. Le conseguenze generate da questi attacchi che risultano sempre più aggressivi, diventano ancora più evidenti. Si vedano ad esempio gli attacchi a danno di strutture pubbliche costrette e bloccare l'operatività quotidiana.

Intanto, non essendo possibile operare una limitazione in senso spaziale della Rete, tale da rendere ardua l'individuazione del locus commissi delicti[337] questo favorisce il proliferare della criminalità, che si nutre del contrasto tra realtà materiale e virtuale,

[336] Rapporto Clusit 2021 – Edizione di ottobre 2021.
[337] S. SEMINARA, *La pirateria su internet e diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997, p. 102.

sfruttando la transnazionalità dell'illecito, la diffusione della condotta e il supposto anonimato che caratterizza la Rete.

Tutte peculiarità che contraddistinguono le condotte criminose messe a segno nel cyberspace, ossia i reati informatici, che coinvolgono modalità operative tecnologicamente avanzate o comunque che incidono su dati, informazioni e programmi.

Le condotte illecite mantengono un distanziamento dagli accadimenti materiali esterni e ciò rende difficile inquadrarle in un campo territorialmente limitato, avendo la possibilità di collocarsi in più luoghi virtuali, venendo meno la necessità di un collegamento tra il soggetto attivo e l'elaboratore informatico[338].

Il numero di truffe favorite dall'informatica e connesse alla pandemia, mediante software maligni, ransomware e attacchi di phishing è aumentato, come abbiamo visto, nel corso della pandemia, prendendo di mira cittadini, imprese e il settore sanitario in particolare, dove nel dark web sono state addirittura scoperte offerte fraudolente di vaccini anti-COVID.

Ad avvalorare questo aspetto interviene anche il Sophos[339] Threat Report 2022 sulla diffusione del ransomware, dedicato proprio al settore sanitario, secondo cui tre aziende su dieci, sono vittime degli hacker. Il 43 % delle organizzazioni attaccate ammette di aver ceduto alla richiesta di riscatto mentre il 57% è riuscito a recuperare i dati ricorrendo al backup. Quest'ultima percentuale scende al 44% nel settore della sanità[340]. Il rapporto riservato sulle strategie della "ransom mafia" parla di 17 miliardi pagati in quattro mesi per impedire ai criminali di bloccare i sistemi aziendali e diffondere le informazioni riservate[341]. Per dare un'idea della dimensione della guerra cibernetica che ha indotto il

[338] R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in Cybercrime a cura di A. Cadoppi, S. Canestrari, A. Manna e A. Papa, Torino, 2019, p. 143.

[339] Sophos è leader mondiale nella sicurezza informatica di nuova generazione, proteggendo più di 500.000 organizzazioni e milioni di consumatori in più di 150 paesi dalle minacce informatiche più avanzate di oggi.

[340] LA STAMPA, *Sanità sotto attacco tre aziende su dieci vittime degli hacker*, 7 agosto 2021, p.20.

[341] CORRIERE DELLA SERA, *Hacker, quali sono le aziende ricattate. Diciassette miliardi pagati in 4 mesi*, 8 agosto 2021, p.9.

governo italiano a costituire un'Agenzia nazionale per la Cybersecurity di raccordo con le nostre agenzie di intelligence, ogni giorno al Soc (Security Operation Center) di Leonardo, a Chieti, si verificano oltre 1500 allarmi di sicurezza, presi in carico e gestiti dagli analisti[342] Il bollettino della criminalità informatica (Cybercrime Judicial Monitor) pubblicato da Eurojust a maggio offre una panoramica degli sviluppi legislativi e della giurisprudenza dell'UE in relazione alla cibercriminalità e ai reati favoriti dall'informatica[343].

La recente ondata di attentati terroristici sul territorio europeo ha ulteriormente sottolineato la necessità di un intervento dell'UE in questo campo. L'attività di gruppi terroristici e traffici illeciti, in particolare quello di sostanze stupefacenti, ormai, come abbiamo visto, corre velocemente sul web. In particolare, si rileva che il quadro delle minacce alla sicurezza informatica sia cresciuto in termini di sofisticazione degli attacchi, complessità e impatto. Questa tendenza sarebbe stimolata da una presenza online in crescita costante, dalla transizione delle infrastrutture tradizionali verso soluzioni online, dall'interconnettività a livello sempre più avanzato e dallo sfruttamento di nuove funzionalità delle tecnologie emergenti nel contesto attuale.

Concludendo si sottolinea come nel cyber, più di ogni altra materia, presente e futuro abbiano un confine labile, per cui è necessario adottare soluzioni flessibili al passo con l'evoluzione tecnologica. L'aumento delle perdite economiche mondiali associate alla cibercriminalità fa emergere l'urgenza di mettere a punto applicazioni e infrastrutture sicure che possano anticipare una minaccia in costante crescita e reagirvi prontamente. C'è da auspicare che il PNRR (Piano nazionale di ripresa e resilienza), che complessivamente destina circa 45 miliardi di euro per la "transizione digitale", possa rappresentare per l'Italia l'occasione di recuperare e colmare le proprie lacune in ambito cyber. Anche nella comunicazione della Commissione al Parlamento europeo e al Consiglio sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza del giugno 2021 si evidenzia come, in tempo di pandemia, la resilienza è più importante che mai nel momento in cui l'infrastruttura sanitaria è già sotto forte pressione e gli incidenti informatici

[342] CORRIERE DELLA SERA, Brevetti e difesa, scudo italiano. Nel bunker digitale di Leonardo, 8 agosto 2021, p.35.

[343] Eurojust, Cybercrime Judicial Monitor, Issue 6 – maggio 2021

mirati a ospedali, organismi medici e servizi sanitari generali possono assumere conseguenze drammatiche. Le conseguenze che le aziende subiscono a causa dei crimini informatici sono sempre più dispendiose e devastanti e sottolineano l'importanza crescente di una pianificazione strategica e un monitoraggio costante degli investimenti in sicurezza.

Dopo la rivoluzione introdotta dal digitale e a seguito di quanto previsto dal nuovo Regolamento UE 679/2016[344] sulla protezione dei dati personali la gestione integrata della sicurezza e della privacy risultano aspetti fondamentali che le aziende devono introdurre accanto all'agilità, alla scalabilità e all'efficienza.

L'avvento del GDPR ha letteralmente sconvolto il mercato digitale perché ha imposto alle aziende per essere compliance, di prestare maggiore attenzione e responsabilità nell'ambito del rischio. Salvaguardare i dati sarà un aspetto imprescindibile per restare sul mercato e aumentare sempre di più competitività e produttività. Particolare attenzione è richiesta sulle modalità con cui raccogliere ed utilizzare i dati dei clienti e sulla scelta delle tecnologie da mettere in campo per garantirne la sicurezza.

Privacy e Security Informatica, due lati della stessa medaglia possiamo dire, offrono un grosso potenziale alle aziende che devono essere pronte ad agire e a sfruttare al meglio il cambiamento a proprio vantaggio con sistemi che stanno modificando profondamente la nostra vita quotidiana, aprendo a nuove opportunità e, allo stesso tempo, ponendo nuove sfide in ambito etico, giuridico e sociale[345]. Per un'azienda non essere protetta in maniera adeguata da attacchi ed infezioni di natura informatica, rappresenterà una nuova forma di "digital divide", con maggiori costi, perdita di reputazione ed esposizione a truffe e, non ultimo, a problemi legali.

La trasformazione digitale se non gestita correttamente rischia di creare seri rischi. Per cui difendere la propria azienda da possibili minacce informatiche è fondamentale

[344] A. BIASIOTTI, *Il nuovo Regolamento europeo sulla protezione dei dati*, EPC Editore, 2018, p. 301. Noto come GDPR (General Data Protection Regulation) approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e applicabile a decorrere dal 25 maggio 2018**.**

[345] G. M. SCHNEIDER, J. L. GERSTING, *Informatica, edizione italiana*, Apogeo, Milano 2007, p.5 e ss.

perché l’impatto di incidenti informatici assume una dimensione significativa, con ricadute economiche e sociali. Di qui la necessità di un’ulteriore crescita degli investimenti in sicurezza informatica. Solamente le imprese che riescono a comprendere da subito il panorama delle minacce e si concentrano sulla sicurezza, costruendo solide basi di difesa, avranno una opportunità maggiore di annullare gli attacchi indesiderati, di individuarli con anticipo e di rispondere in maniera efficace incrementando la produttività.

CONCLUSIONI

La cybersecurity è divenuta oramai un'emergenza a livello globale. La pandemia di Covid-19 ha prodotto, come effetto collaterale, un'accelerazione del processo di digitalizzazione delle imprese, palesando al contempo impreparazione e vulnerabilità del sistema. La ricca casistica di attacchi cibernetici di questi ultimi anni, di cui si è parlato ampiamente in questo elaborato, mostra che è necessario che maturi, ancor di più, nella classe imprenditoriale e tra le Istituzioni, una consapevolezza diffusa delle problematiche legate alla cybersecurity.

È pur vero che l'emergenza ha rappresentato, nonostante tutto, una grande opportunità per innalzare i livelli della qualità dell'infrastruttura informatica nazionale degli Stati membri. La pandemia ci insegna che nessuno può ritenersi invulnerabile e nessuna azienda o Pubblica Amministrazione può ritenersi esclusa dal rischio di un attacco. L'irrompere della tecnologia informatica ha messo in evidenza, da un lato, la potenzialità di tale fenomeno, e dall'altro, la vulnerabilità dei fruitori esposti in rete.

In questi ultimi anni di emergenza sanitaria sono state poste in essere limitazioni senza precedenti sulla libertà di circolazione e gli Stati hanno reagito riprendendo il controllo sulle proprie frontiere, disponendo deroghe e modifiche sostanziali alle regole legate alla concorrenza e agli aiuti di Stato. Anche i limiti della competenza della UE in tema di tutela della salute e sanità pubblica sono emersi con vigore e hanno inciso sulla sua capacità di reazione.

L'impatto sugli ordinamenti degli Stati membri è stato forte e non ha risparmiato attacchi a strutture sanitarie e alla ricerca.

In questo grande spazio pubblico che è Internet, definito «il più grande che l'umanità abbia conosciuto, la rete che avvolge l'intero pianeta»[346], potenzialmente incontrollato, i giuristi si trovano continuamente di fronte a nuove sfide, alla necessità di un continuo adeguamento e ripensamento dei paradigmi e delle categorie tradizionali del diritto e

[346] S. RODOTÀ, "*Una costituzione per internet*?", in Politica del diritto, fascicolo 3, settembre 2010, Il Mulino rivista web, p.338.

all'esigenza, sempre più pressante, di garantire la tutela dei diritti fondamentali della persona, soprattutto nel contesto tecnologico in continua trasformazione.

L'UE lavora su diversi fronti per rafforzare la resilienza informatica, con un quadro regolamentare e operativo in costante evoluzione. Un insieme di norme che comunque rende l'Europa una delle aree più avanzate al mondo di protezione e contrasto alla cyber criminalità.

L'accelerazione digitale impressa dal lockdown ha aumentato esponenzialmente la vulnerabilità alle minacce informatiche di aziende e Stati e la crisi scatenata dall'epidemia sta mettendo in discussione le misure previste dalla programmazione Ue 2021-2027 vista la preoccupante escalation delle intrusioni in rete. Un programma ambizioso, concepito in un momento storico completamente diverso e che oggi potrebbe essere messo in discussione.

Nel periodo di emergenza sono state realizzate campagne informative incentrate per lo più su tematiche COVID, magistralmente coordinate da cyber criminali che giorno per giorno hanno trasformato le piazze virtuali in grossi contenitori di minacce informatiche.

Lo smart working, quale misura di contenimento dei contagi e nell'evoluzione in modalità telematica delle azioni di socializzazione, ha generato inevitabilmente un vulnus nei sistemi di sicurezza informatica, ampliando la 'superficie d'attacco'.

Con la recente attribuzione a Bucarest dello European Cybersecurity Competence Centre, l'Unione Europea ha dato un ulteriore slancio alla sua azione in tale ambito. Solo due anni dopo la sua entrata in vigore, la direttiva NIS (sicurezza delle reti e dei sistemi informativi) subisce un'importante revisione con un'ulteriore proposta presentata dalla Commissione. Nuovi requisiti e obblighi sono dettati per i service providers, quindi, più potere alle autorità nazionali per assicurare il rispetto della normativa, fino alla sospensione temporanea delle attività imprenditoriali.

Sullo sfondo, la nuova Strategia sulla Cybersecurity consentirà a imprese e autorità pubbliche di scambiare informazioni su minacce e possibili risposte, attraverso la creazione di un vero e proprio scudo, il c.d. "Cyber Shield", usufruendo di centri territoriali che utilizzano strumenti di intelligenza artificiale.

Abbiamo visto come la Commissione nell'immediato abbia deciso di fare della sicurezza informatica una priorità attraverso la sua proposta per un nuovo Digital Europe Programme (DEP): due miliardi di euro su un totale, per l'intero programma, di 9,2 miliardi

destinati a soluzioni ottimali di sicurezza, a rinforzare le funzionalità degli Stati membri e al settore privato per migliorare reti e sistemi informativi nonché a sostenere tecnologie digitali avanzate industriali.

Il Digital Europe Programme e Horizon Europe metteranno a disposizione risorse importanti per i prossimi 7 anni a cui si aggiungerà l'investimento degli Stati membri. Indubbiamente, si tratta di una prima decisa risposta in uno scenario in cui viene evidenziato anche il divario digitale e il bisogno di rafforzare l'istruzione digitale.

Nel frattempo però abbiamo una grandissima occasione: il PNRR e i fondi che saranno riversati in innovazione digitale nei prossimi anni.

Il piano per la ripartenza europeo, con i 1840 miliardi di Next Generation EU e del nuovo bilancio pluriennale, assume un ruolo di rilievo nella transizione digitale accompagnata dalla strategia per la cybersicurezza.

Il vero pilastro nel contrasto al cybercrime resta la Convenzione di Budapest anche se sono intervenuti successivamente la direttiva Nis e il Regolamento generale sulla protezione dei dati personali che hanno dettato obblighi di compliance con sanzioni molto incisive agli operatori essenziali e alle imprese.

Il regolamento 2019/881, c.d. Cybersecurity Act, invece, nell'ambito della strategia nazionale per la sicurezza della rete e dei sistemi informativi definita dalla Direttiva NIS, ha avuto l'obiettivo di realizzare un quadro europeo per la certificazione della sicurezza informatica dei prodotti e dei servizi digitali, in base ad un modello di security by design, rafforzando il ruolo dell'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza. Una logica diversa rispetto a quella che anima il sistema previsto dal d.lgs. 231/2001 anche se tuttavia, a vent'anni dall'emanazione del decreto legislativo, sono ancora troppo poche le imprese dotate di modelli organizzativi idonei.

Infine, il decreto-legge n. 105 contenente "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" introduce misure volte ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle PA, degli enti e degli operatori nazionali, pubblici e privati.

Altro elemento portante, come è emerso, è la creazione di un'Agenzia europea per la cybersecurity (ENISA) con l'obiettivo di supportare gli stati membri, le istituzioni europee e gli altri stakeholder nella lotta ai cyber attacchi.

L’altra direttrice sulla quale si muove con decisione l’Unione Europea è quella dell’Intelligenza Artificiale poiché il suo utilizzo in vari prodotti e servizi può far sorgere rischi non esplicitamente coperti dalla legislazione europea.

Ma una delle maggiori sfide con cui si dovrà confrontare la Commissione nel contrasto alla cyber criminalità è l’adozione del 5G, su cui si fonda lo sviluppo proprio di cloud e Intelligenza Artificiale. Un mercato in grado, secondo le stime, di generare redditi a livello globale con benefici concentrati su 4 settori strategici come auto, sanità, trasporto ed energia.

Forme nuove e sempre più diverse e sofisticate di minacce cibernetiche emergeranno quanto più si svilupperà la tecnologia legata a “Internet of things”, big data e, nel prossimo futuro, quella collegata all’Intelligenza Artificiale.

È quindi facile comprendere l’importanza sempre crescente che la cyber security assumerà nel prossimo futuro.

Il passaggio all’Internet of things ha di fatto digitalizzato ogni aspetto della vita quotidiana, moltiplicando esponenzialmente il volume dei dati personali trattati che circolano in rete senza filtro. Di qui anche l’esigenza impellente di tutelare i dati personali in rete, tentando di garantire il rispetto della dignità, dell’identità e della riservatezza della persona.

Viene in rilievo, quindi, la proiezione sociale del diritto alla privacy, quale diritto non tanto alla segretezza, ma al controllo dei propri dati personali in rete, alla diffusione consapevole degli stessi e alla necessità di prevenire un trattamento illecito degli stessi.

Così la cybersecurity ha focalizzato su di sé l’attenzione del mondo accademico sempre più proteso sulle attività di Cyber Threat Intelligence e Threat Hunting.

Abbiamo voluto approfondire in questo lavoro il contesto della Cybersecurity a livello europeo attraverso analisi e report pubblicati in materia identificando le numerose minacce provenienti dal cyberspace e analizzando l’impatto a livello economico e sociale.

Il rapporto Clusit 2021 ci ha restituito una fotografia digitale dell’annus horribilis 2020 confermata ampiamente anche nel primo semestre 2021: l’Italia collocata al 20esimo posto nel ranking complessivo dei 27 Paesi UE (con a capo la Danimarca), risulta ancora penultima tra Paesi più popolosi, davanti solo alla Polonia e con forti lacune sugli indicatori legati alle competenze digitali.

Le perdite sono ingenti. Anche nel Rapporto Europol 2021(IOCTA) emerge un quadro sulla digitalizzazione accelerata dalla emergenza sanitaria.

Gli attacchi più diffusi sono ancora di tipo Malware con il 43% del totale (+10,5%). Il 25% degli attacchi sono stati indirizzati verso l'Europa.

Questo potrebbe essere riconducibile a due diversi fattori e non tanto alla maggiore attenzione verso il nostro continente rispetto ad altri. Il primo fattore potrebbe essere il GDPR che impone alle aziende vittime di attacchi di denunciare il reato, pena pesanti sanzioni. In seconda ipotesi, la pandemia è la causa indiscussa di un aumento esponenzialmente del numero di attacchi.

L'aspetto più preoccupante è rappresentato dall'incremento dell'attività dei ransomware, con relativa richiesta di riscatto, che provengono da organizzazioni di dimensioni sempre più elevate.

Dunque, come affrontare nel prosieguo la problematica? Se è vero che cresce la spesa in sicurezza informatica è altrettanto vero che si fa ancora troppo poco per tutelare le aziende dal rischio cyber.

Da qui l'esigenza di agevolare gli investimenti in cybersecurity, rendendoli meno onerosi possibile attraverso appositi sgravi fiscali per le imprese che investono e producono nel settore, incentivando una diffusa awareness (grado di conoscenza) per guardare al futuro senza timore.

Sarà importante investire sulla formazione, sull'innovazione tecnologica, sulle competenze per rendere il nostro Sistema un Paese sicuro, pragmatico ed efficiente così come è assolutamente necessario uniformare le leggi in ambito Ue.

Da questa analisi ne deriva che occorre proprio un'aperta condivisione, perché solo maturando questa consapevolezza si potranno mettere a fattor comune informazioni ed esperienze per investimenti mirati in sicurezza informatica e tecnologie digitali avanzate. Due fattori risulteranno determinanti sulle prospettive future: la risposta che l'UE saprà fornire per rilanciare la ripresa dopo l'emergenza COVID e la capacità dei Governi dei 27 Stati membri a trovare una mediazione nella definizione di risorse e contenuti della prossima programmazione.

BIBLIOGRAFIA

A. ADAM, TIZZANO A., *Lineamenti di diritto dell'Unione europea*, Giappichelli Editore, Torino.

ACCONCI P., BARONCINI E.*, Gli effetti dell'emergenza Covid-19 su commercio, investimenti e occupazione.* Una prospettiva italiana (a cura di), Dipartimento di Scienze giuridiche, Università Bologna, luglio 2020.

ALESSANDRI A., SEMINARA S., *Diritto penale commerciale*, Vol. I, I Principi generali, G. Giappichelli Editore, 2018.

AMATO G., DESTITO V.S., DEZZANI G., SANTORIELLO C., *I reati informatici*, Cedam Milano.

ARAGONA V., *La tutela penale della privacy nel cyberspazio*, in Rivista di diritto penale contemporaneo. Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione, Editore Associazione "Progetto giustizia penale", 2019.

BALDONI R., DE NICOLA R., PRINETTO P., (a cura di), *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici,* Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l'Informatica, 2018.

BALDUCCI ROMANO F., *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia*, in Rivista italiana di diritto pubblico comunitario, 2015.

BALLONI A., BISI R., SETTE R., *Principi di criminologia applicata,* Cedam, 2015.

BARBERA A., *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di Giustizia,* in Rivista AIC, n. 4/2017.

BARBERA A., *Art. 2 Costituzione,* in Principi fondamentali (artt. 1-12), Commentario della Costituzione, Branca G. (a cura di). Zanichelli Editore, Bologna-Roma, 1975.

BARRESI F., NIGRETTI M., Fenomeno Hacking. *Analisi sociocriminalistica dell'intrusione informatica*, Iris4 Edizioni, Roma, 2012.

BERNARDI A.**,** *L'armonizzazione delle sanzioni in Europa: linee ricostruttive,* in 'Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale', Grasso G. - Sicurella R. (a cura di), Milano, 2008.

BERTOLOTTI C., *Il terrorismo in Europa, Francia Germania e Italia: tra attacchi, contrasto ed espulsioni,* Trimestrale società italiana per l'organizzazione internazionale. Nuove forme di estremismo: strumenti di prevenzione e contrasto delle minacce, Editoriale Scientifica.

BERTOLOTTI C., I*mmigrazione e terrorismo. I legami tra flussi migratori e terrorismo di matrice jihadista*, Lugano, 2020.

BIASIOTTI A., *Il nuovo Regolamento europeo sulla protezione dei dati,* EPC Editore, 2018, p. 301.

BIFULCO R., *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno.* Diritto Pubblico Europeo - Rassegna Online.

BIGNAMI M., *Costituzione, Carta di Nizza, CEDU e legge nazionale: una metodologia operativa per il giudice comune impegnato nella tutela dei diritti fondamentali*, in Rivista AIC, n. 1/2011.

BRANDEIS L.D., WARREN S., *The Right to Privacy*, in 4 Harward Law Review, 1890.

BRIGHI R., "*La vulnerabilità nel cyberspazio*", in Ars interpretandi, 2017, n. 1.

BROTHERSTON V.L., BERLIN A., VISCARDI R. (Traduttore), *La sicurezza dei dati e delle reti aziendali. Tecniche e best practice per evitare intrusioni indesiderate*, O'Reilly, 2018.

BRUNNER J., *The Shockwave Rider Harper Row*, Harper & Row, 1975.

BUTTARELLI G., *Banche dati e tutela alla riservatezza*, Giuffrè. Milano, 1997.

CAGGIANO G., *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in Studi sull'integrazione europea, 2018.

CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008.

CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93* (convertito con modificazioni dalla L. 15 ottobre 2013, n.119), in Cass. Pen., 2014.

CALIFANO L., COLAPIETRO C. (a cura di*), Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali. Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017.

CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli, 2016

CALINGIURI M., *Cyber Intelligence. Tra libertà e sicurezza*, Donzelli Editore, 2016.

CANNIZZARO E., *Il diritto dell'integrazione europea. L'ordinamento dell'Unione,* Seconda edizione, Torino, Giappichelli, 2017.

CARACCIOLI I., *I soggetti del diritto penale: evoluzione delle categorie dagli anni Cinquanta ad oggi*, in dir.pen. XXI secolo, 2005.

CARMONA A., *Premesse a un corso di diritto penale dell'economia*, Cedam, 2002.

CARNELUTTI F., *Diritto alla vita privata*, Riv. trim. dir. pubbl., 1955.

CAROTTI B. *La collaborazione tra autorità europee delle telecomunicazioni*, Esperia, London, 2011.

CARTABIA M.*, L'ora dei diritti fondamentali nell'Unione Europea*, in I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Bologna, Il Mulino, 2007.

CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in LOSANO (a cura di), La legge italiana sulla privacy. Un bilancio dei primi cinque anni, Roma-Bari, 2001.

CASSANO G., SCORZA G., VACIAGO G. (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione e giurisprudenza*, Cedam, Padova, 2012.

CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in Eur. dir. priv., 1998.

CERRI A., *Riservatezza (diritto alla)*, II, Diritto comparato e straniero», in Enc. giur., Roma, 1991.

CICCIA MESSINA A., *Guida al codice privacy. Come cambia dopo il GDPR e il D.Lgs. n.101/2018*, Wolters Kluwer, Milano, 2019, Prefazione.

COSTABILE G., *Computer forensic e informatica investigativa alla luce della l. n. 48 del 2008*, in Cyberspazio e diritto, Vol. 11, 2010, n. 3.

CRESPI S., *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in Rivista Italiana di diritto pubblico comunitario, 2015.

CURIONI A., *Il giorno del Bianconiglio,* Chiarelettere Editore, 2021.

D'AGOSTINO L., *La tutela penale dei dati personali nel riformato quadro normativo un primo commento al D Lgs.10 agosto 2018, n.101,* in Arch. pen. web, 2019.

DE CUPIS A., *Il diritto alla riservatezza esiste,* in Foro it., IV, 1954.

DEMURO G., *La Carta dei diritti,* in Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea, Lucarelli A., Patroni Griffi A. (a cura di), Napoli, Edizioni Scientifiche Italiane, 2009.

DEZZANI G., PICCINNI M.L., *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs, n.231 del 2001*, in Resp.amm. soc.ed enti, 2011, Plenum.

DEZZANI G., *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica, in La responsabilità amministrativa delle società e degli enti,* Rivista 231, 2010.

DI MASCIO F., ANGELETTI S., NATALINI A., *Lo smart working nelle pubbliche amministrazioni centrali ai tempi del COVID – 19,* Rivista Italiana di Politiche Pubbliche, Il Mulino, 1/2021, aprile.

DI RESTA F., *La nuova "privacy europea. I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori*, G. Giappichelli Editore, 2018.

ERDOS D., *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in Journal of Law and Society, 2016.

FEDELI P., RICCI G., CORTUCCI C., *Lineamenti di Criminologia, Napoli*, ESI, 2006.

FERRARO F., LAZZERINI N., *Commento all'art. 52 CdfUE, (a cura di)* R. MASTROIANNI, POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O., Carta dei diritti fondamentali dell'Unione europea, 2017.

FLOR R., "*Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*", in *Diritto di Internet*, 2019, n. 3.

FLOR R., *Cyber-terrorismo e diritto penale in Italia*, in, Diritto penale e modernità. Nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, Napoli, 2017.

FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in Cybercrime a cura di A. Cadoppi, S. Canestrari, A. Manna e A. Papa, Torino, 2019.

FLOR R., *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente,* in Rivista italiana di diritto e procedura penale, 2007, Giuffrè.

FLORA G., *Il furto di identità*, in AA.VV., Sicurezza e privacy: dalla carta ai bit (a cura di COSTABILE), Esperta Edizioni, 2005.

FRANCHINA A., *Spunti di riflessione sul delitto di illecito trattamento di dati personali: reato istantaneo o permanente?* in Giurisprudenza Penale Web, 2020.

FREDIANI C., *Cybercrime. Attacchi globali, conseguenze locali*, Hoepli, 2019.

FULVI F.R., *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica,* in dir. Pen. proc., 2009, p. 639 e ss.; F. Modugno, Ordinamento giuridico, in Enc. Dir., XXX,1980.

GIORDANO M.T., VACIAGO G., "*La sicurezza informatica, un asset aziendale strategico*", Milano, 2018, pp. 273-283.

GRANIERI M., *Il sistema della tutela dei diritti nella legge 675/1996*, in AA. VV., Diritto alla riservatezza e circolazione dei dati personali, (a cura di Pardolesi), Milano, 2003, p. 437 ss.

GRAY C.S., *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling, Strategic Studies Institute*, Carlisle PA, April 2013.

GUTWIRTH S., LEENES R., DE HERT P. (edited by), Reforming european data protection law, law, governance and technology series, XX, SPRINGER, 2015.

HAAS J., NEELY J.C., "Central Bank Responses to COVID-19," Economic Synopses, No. 23, 2020.

IASELLI M., *Manuale operativo del D.P.O. (Data Protection Officer)*, Maggiol, Rimini, 2018.

JEAN C., SAVONA P., *Intelligence Economica*, Rubbettino, 2011.

KOOPS B.J., ADAMS S. ET AL., *The governance of cybersecurity, Tilburg University TILT* - Tilburg Institute for Law, Technology, and Society, 2015.

KRAEHENMANN S., '*Foreign Fighters under International Law*', Academy Briefing No 7, Geneva Academy of International Humanitarian Law and Human Rights, October 2014.

KREMLING J., SHARP PARKER A.M., *Cyberspace, Cybersecurity, Cybercrime*, Sage pubblication, 2018.

LATTANZIO G., SEVERINO P. (a cura di), *Responsabilità da reato degli enti,* vol.II, Diritto processuale, G.Giappichelli editore, 2020.

LATTANZIO G., SEVERINO P. (a cura di), *Responsabilità da reato degli enti*, vol.I, diritto sostanziale, G.Giappichelli Editore, 2020.

LIOTTA A., *Una spinta verso la trasformazione tecnologica delle imprese: l'iperammortamento come strumento di politica fiscale per l'innovazione*, Luiss Law Review, 2017.

LISI F., MURANO G., NUZZOLO A., *I reati informatici*, Maggioli editore, 2004.

LOSANO M.G., *La legislazione tedesca sulla protezione dei dati individuali*, in ALPA-BESSONE, *Banche dati telematica e diritti della persona*, Padova, 1984.

MACARIO F., *La protezione dei dati personali nel diritto privato europeo*, in CUFFARO, RICCIUTO (a cura di), La disciplina del trattamento dei dati personali, Torino, 1997.

MARCHESE C.*, Il ruolo dello stato a fronte dell'emergenza pandemica e le risposte elaborate in sede europea: la garanzia dei diritti ed il rilancio economico alla luce del rapporto tra condizionalità e solidarietà, A*IC (Associazione italiana costituzionalisti) Rivista N°: 1/2021.

MARINUCCI G., DOLCINI E., *Manuale di diritto penale*, Milano, Giuffrè, 2015.

MARKOPOULOU D., PAPAKONSTANTINOU V., HERT P., *The Nis Directive, Enisa's role and the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019.

MAZURIER P.A., *Sul concetto di Cyberterrorismo e la Costruzione della Cyber(in)sicurezza*, Center for Cyber Security and International Relations Studies, Firenze, 2017.

MONNET J., *Mémoires*, Paris, Fayard, 1976.

MONTAGNANI M.L., CAVALLO M.A., *Cybersecurity and liability in a Big Data World*, in Market and Competition Law Review, 2018.

MOSCO G.D., *La collaborazione tra imprese per la sicurezza informatica*, Luiss Law Review, 2017.

MUKHOPADHYAY A., PRAJWAL A., *A robust framework for prevention of cyber attacks in the Covid era,* 2a Conferenza Internazionale per le Tecnologie Emergenti, INCET 2021.

MUNARI F., CALZOLARI L., *Le regole del mercato interno alla prova del COVID19: modeste proposte per provare a guarire dall'ennesimo travaglio di un'Unione incompiuta,* in Eurojus, Speciale 2020;

OCONNELL J., *10 Most Notorious Hackers of All Time*, hacked.com, 3 settembre 2015.

PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in Studi in onore di F. Antolisei, II, Milano, 1965.

PALLA T.G., TAYEB S., *Intelligent Mirai Malware Detection for IoT Nodes. Electronics*, Academic Editor: Taeshik Shon, 24 May 2021.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in Diritto alla riservatezza e circolazione dei dati personali, a cura di Pardolesi, Milano, 2003.

PARODI C., CALICE A., *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001.

PECORELLA C., *Reati informatici*, in Enc. Dir., Annali, X, Milano, 2017.

PEDRAZZI M., *Artt. 6-7 TUE*, in Commentario breve ai trattati dell'Unione europea, F. POCAR, M.C. BARUFFI (a cura di), II edizione, Padova, Cedam, 2014.

PENNAROLA F., *Innovazione e Tecnologie Informatiche,* Università L. Bocconi Editore, 2006.

PESTELLI G., *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico*, in Cass. Pen., 2012.

PETRINI D., *La responsabilità penale per i reati via internet*, Jovene, 2004.

PICOTTI L., *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. GRASSO, L. PICOTTI, R. SICURELLA, (a cura di). *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano 2011.

PIERGALLINI V., *I reati presupposto della responsabilità dell'ente e l'apparato sanzionatorio, in AA.VV., Reati e responsabilità degli enti*. Guida al d.lgs. 8 giugno 2001, n.231, Giuffrè, 2010.

POCAR F., TAMBURINI M., *Norme fondamentali dell'Unione europea***,** Giuffrè Editore, 2010.

POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE*, in (a cura di) MASTROIANNI R., POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O., Carta dei diritti fondamentali dell'Unione europea, Giuffrè, 2017.

POLLICINO O., *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in Rivista diritto dei media, 2018.

RACHMAN V.G., "The Perverse Political Effects of Covid-19", Financial Times, 29 dicembre 2020.

RAMPINI F., *La seconda guerra fredda*. Lo scontro per il nuovo dominio globale, Mondadori, 2019.

RAPICAVOLI R., Come applicare il GDPR e il codice privacy negli studi e nelle aziende, Maggioli, Rimini, 2018.

RESTA G., *Il diritto alla protezione dei dati personali*, in CARDARELLI-SICA-ZENO ZENCOVICH, *Il codice dei dati personali*, Milano, 2003.

RODOTÀ S., "*Una costituzione per internet*?", in Politica del diritto, fascicolo 3, settembre 2010, Il Mulino rivista web.

RODOTÀ S., *Intervista su privacy e libertà*, a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005.

ROMASHKINA N.P., ZAGORSKI A.V., *Information security threats during crises and conflicts of the XXI century* 2016, Moscow.

ROSSI DAL POZZO F., *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679*, in Eurojus, 2018.

ROSSI F., Luci ed ombre sull'intervento dell'unione europea a fronte dell'emergenza del Covid-19, in Nomos, 2020.

RUIZ-JARABO COLOMER D., Avvocato generale, punto 39 delle conclusioni rese l'8 aprile 2008 in causa C-297/07, Bourquain, in Raccolta.

SALERNO G.M., *La protezione della riservatezza e l'inviolabilità della corrispondenza, in I diritti costituzionali*, R. Nania, P. Ridola (a cura di), vol. 2, Torino, Giappichelli, 2006.

SALVATORE V. *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato Unione Europea,* Studio EPRS | Servizio Ricerca del Parlamento europeo Unità Biblioteca di diritto comparato PE 628.243, Ottobre 2018 IT, Segretariato generale del Parlamento europeo.

SARZANA DI S. IPPOLITO C., *La legge di ratifica della convenzione di Budapest*, in Dir. Pen.Proc., 2008.

SCHNEIDER G.M., GERSTING J.L., *Informatica*, edizione italiana, Apogeo, Milano 2007.

SCIAUDONE R., CARAVÀ E., *Il codice della privacy*, Commento al D.LGS. 30 giugno 2003, n.196 e al D.LGS. 10 agosto 2018, n.101 alla luce del Regolamento (UE) 2016/679 (GDPR), Prefazione, Pacini giuridica, Pisa, 2019.

SEMINARA S., *La pirateria su internet e diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997.

SICA S., Verso *l'unificazione del diritto europeo alla tutela dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di Sica-D'Antonio-Riccio, Cedam, Milano, 2016.

SOTIS C., *Il trattato di Lisbona e le competenze penali dell'unione europea*, in *Cass. pen*., n. 3-2010.

TESSARO T., C*ome cambia la trasparenza amministrativa dopo il Gdpr e il nuovo decreto privacy*, Maggioli, Rimini, 2019.

TETI A., C*yber intelligence e cyber espionage come cambiano i servizi di intelligence nell'era del cyber spazio,* in «Gnosis», Rivista italiana di intelligence, 3/2013.

TIRINO N., *Cambridge Analytica. Il potere segreto, la gestione del consenso e la fine della propaganda*, Lecce, Libellula Edizioni, 2019.

VANNI D., «Protezione dei dati personali (dir. civ.)», in *Digesto/civ*., *Agg*., Torino, 2013.

VISCONTI A., *La sicurezza informatica e la rete*, in G. Cassano (a cura di), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, Wolters Kluwer, Milano, 2017.

VON SOLMS R., VAN NIEKERK J., "*From information security to cyber security*", in Computers &security, 2013, n. 38.

WYLIE C., *Il mercato del consenso: come ho creato e poi distrutto Cambridge Analytica*, Milano, Longanesi, 2020.

ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in RESTA G. e ZENO-ZENCOVICH V. (a cura di), La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy Shield", Roma, 2016.

QUOTIDIANI CONSULTATI

ANSA, *Cyber-attacco all'Ema, obiettivo il vaccino Pfizer*, Roma, 10 dicembre 2020.

CORRIERE DELLA SERA, *Blackout di Facebook sale Snapchat*, 7 ottobre 2021.

CORRIERE DELLA SERA, *Brevetti e difesa, scudo italiano*. Nel bunker digitale di Leonardo, 8 agosto 2021.

CORRIERE DELLA SERA, *Gli hacker attaccano l'ospedale, caos al pronto soccorso*, di Rinaldo Frignani ,14 settembre 2021.

CORRIERE DELLA SERA, *Gli hacker nel frigorifero*, di Federico Cella, 23 ottobre 2016.

CORRIERE DELLA SERA, *Hacker mobilitati per le elezioni USA*, di Massimo Gaggi, 5 luglio 2019.

CORRIERE DELLA SERA, *Hacker, dati e stipendi a rischio. Ora i pm indagano per terrorismo*, di Rinaldo Frignani, 4 agosto 2021.

CORRIERE DELLA SERA, *Hacker, quali sono le aziende ricattate. Diciassette miliardi pagati in 4 mesi*, 8 agosto 2021.

IL MESSAGGERO, *Hacker, la minaccia ci aspetta in albergo*, di Francesco Malfetano, 8 luglio 2019.

IL SOLE 24 ORE, *La cybersecurity tra gli affari di Borsa*, 6 agosto 2021.

IL SOLE 24 ORE, *Un salto di qualità per battere le cyberwar*, di Alessandro Curioni, 20/8/2021.

IL SOLE 24ORE, *I furti e le rapine crollano con il virus ma più reati sul web*, di M. Casadei e M. Finizio, 26 ottobre 2020, https://www.ilsole24ore.com/art/i-furti-e-rapine-crollano-il-virus-ma-piu-reati-web-AD7B5Px.

LA REPUBBLICA, *Abusi e monopolio la grande crisi di Facebook oltre il black out*, di Federico Rampini, 6 ottobre 2021.

LA REPUBBLICA, *Attacco hacker ai dati del Lazio. Stop ai vaccini, chiesto un riscatto*, di Arianna Di Cori e Romina Marceca. 2 agosto 2021.

LA REPUBBLICA, *Attacco Wannacry così Trump accusa Pyongyang*, di Federico Rampini, 20 dicembre 2017.

LA REPUBBLICA, *Dopo il riscatto alla Regione Lazio, hacker violano un server della sanità Toscana*, 20 agosto 2021.

LA REPUBBLICA, *I guai della galassia Zuckerberg. Fb e Whatsapp bloccati per ore*, di Raffaella Menichini, 5 ottobre 2021.

LA REPUBBLICA, *Petya, l'ultimo attacco hacker mondiale*, di Rosalba Castelletti, 28 giungo 2017.

LA STAMPA, *Caccia agli hacker. "I dati sono salvi" Nominato Baldoni*, di Edoardo Izzo, 6 agosto 2021.

LA STAMPA, *Chi sono i pirati della cyberguerra*, di Gianni Riotta, 23 ottobre 2016.

LA STAMPA, *Covid, sette attacchi hacker ai server di AstraZeneca*, di E. Izzo, 30 dicembre 2020.

LA STAMPA, *Sanità sotto attacco tre aziende su dieci vittime degli hacker*, 7 agosto 2021.

QUOTIDIANO SANITÀ, *Roma. Attacco hacker all'ospedale San Giovanni. Ma nessun blocco delle attività cliniche*, 13 settembre 2021.

SITOGRAFIA

www.europarl.europa.eu

www.consilium.europa.eu/it

www.cert-agid.gov.it

www.interno.gov.it

www.eunews.it

www.consilium.europa.eu/it

www.camera.it

www.eur-lex.europa.eu/

www.edpb.europa.eu

www.ec.europa.eu/health

www.rivista.eurojus.it

www.innovazione.gov.it

www.enisa.europa.eu

www.lavoro.gov.it

www.protezionedatipersonali.it

www.cybersecurity360.it

www.rainews.it

www.ilsole24ore.it

www.penaledp.it

www.ec.europa.eu

www.antiriciclaggiocompliance.it