amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 3/2021
ESTRATTO

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, José Manuel Ruano de la Fuente, Francesco Rota, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Sergio Contessa, Mariaconcetta D'Arienzo, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Gaetano Natullo, Carmen Pérez González, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"

di Bianca Nicla Romano

(Dottore di ricerca, Università "Federico II" di Napoli)

Sommario

1. Premessa; 2. Digitalizzazione e *cybersecurity*; 3. L'identità digitale e la sua tutela giuridica; 4. Il preoccupante fenomeno del "furto di identità digitale"; 5. Lo *spear phishing* ed il *social engineering, vulnera* ai sistemi informatici; 6. Il *phishing* e la sua disciplina come fattispecie delittuosa; 7. La tutela delle identità virtuali nel Codice per la Protezione dei Dati Personali; 8. L'attività della Pubblica Amministrazione e le conseguenze degli attacchi informatici tra difficoltà di prevenzione e gestione; 9. Le prospettive di riforma della *cyber*sicurezza contenute nel PNRR; 10. I recentissimi interventi normativi in materia di sicurezza informatica a livello europeo e nazionale; a) Il Regolamento (UE) 2021/887 istitutivo del Centro Europeo di competenza per la cybersicurezza; b) La Legge 109/2021 istitutiva dell'Agenzia per la *cyber*sicurezza nazionale; 11. Considerazioni conclusive

Abstract

This essay examines the most frequent and best-known types of cyber-attacks and addresses the impact they have on the information systems of companies, private citizens and, of course, of the Public Administration, particularly in terms of the management and protection of both digital identity and personal data. This analysis shows that investments in information security and digital literacy are still inadequate and fragmentary, as well as the regulatory instruments: both those specifically related to individual criminal offences, and those related to the actions necessary to prevent and fight them, since they are not yet implemented in a joint and consolidated manner among States and the various institutional actors. Therefore, the reform perspectives embodied in the PNRR will be analyzed, together with the most recent regulatory acts at European and national level, namely Reg. (EU) 2021/887 and the Italian law 109/2021 which finally establishes the National Cybersecurity Agency in Italy.

ISSN 2036-7821

1. Premessa.

Quanto attualmente caratterizza la nostra società in termini di innovazione tecnologica e di progresso costituisce un risultato assolutamente impensabile in passato; si potrebbe dire che sia tutto accaduto nel giro degli ultimi due decenni in particolare, ma, in realtà, già dagli anni Trenta del secolo scorso costituiva una ambiziosa aspirazione l'idea di riuscire a riorganizzare la conoscenza in maniera da potere rendere più efficiente ed immediata la selezione delle informazioni. Col tempo, tale aspirazione ha portato a quello che oggi chiamiamo *digitalizzazione* e che è il risultato di un percorso in continua evoluzione, in cui strumenti come gli ipertesti, i *personal computer*, la rete digitale e, dunque, *Internet* hanno sempre più rapidamente preso il sopravvento nella vita quotidiana. Essi sono la testimonianza di un incredibile progresso tecnologico che ha semplificato ed agevolato la realtà in senso generalizzato (e quindi sia rispetto alla Pubblica Amministrazione che rispetto ai privati cittadini) e che, in un momento difficile e drammatico come quello che si è vissuto dagli inizi del 2020 e a causa della pandemia da Covid-19, hanno reso possibile continuare a vivere le proprie vite nonostante il distanziamento.

Volenti o nolenti, siamo tutti travolti da quello che *Internet*, ma anche i *social network*, rappresentano; essi hanno soppiantato completamente i *media* tradizionali come la stampa, la radio ed anche la stessa TV - che, pur essendo ancora largamente utilizzati, appaiono quasi "primitivi" al confronto - perché consentono l'indubbio ed accattivante vantaggio di interagire nonostante la distanza, trasformando l'utente da spettatore passivo a produttore lui stesso di informazioni che, grazie alla rete digitale, si diffondono con una estrema velocità. La realtà è stata modificata al punto da essere ormai prevalentemente caratterizzata da rapporti virtuali in luogo di quelli fisici, e il *cyber*spazio è divenuto il luogo in cui è possibile ritrovare tutto ciò che occorre nella vita quotidiana ed a cui si accede semplicemente grazie ad un *clic* su di un *link*, ovvero su un "collegamento", su una porta di accesso a mondi, informazioni e realtà che si riesce a conoscere, scrutare e scegliere di condividere pur senza viverli fisicamente.

Tali innovative opportunità hanno totalmente trasformato l'agire sociale, la trasmissione della conoscenza ed anche la produzione delle informazioni, conferendo al mercato una fisionomia assolutamente diversa rispetto al passato e che ha, inevitabilmente, influenzato anche il rapporto tra *producer* e *consumer*. La globalizzazione dei rapporti all'interno del mercato virtuale rende l'uomo un consumatore "digitale" che, grazie alla rete, vive ed interagisce nella società della connessione, in cui tutto è condiviso, in cui valgono le stesse forme di comunicazione e di linguaggio ed in cui è possibile utilizzare, per infinite funzioni, un unico mezzo, divenuto elemento essenziale della formazione culturale innanzitutto delle giovani generazioni, ma a cui si sono dovute adeguare (non solo per necessità) anche quelle meno giovani, "travolte" da questo cambio radicale di abitudini e di consumi che ha

investito tutte le attività quotidiane, da quelle lavorative, a quelle di studio, a quelle di svago.

Ci si trova di fronte, insomma, ad una incredibile evoluzione culturale, più *smart* e, quindi, più rapida, che si è realizzata grazie alla trasposizione della vita reale e dei rapporti umani nella realtà della rete digitale, superando l'aspetto *statico* dell'informazione che ha caratterizzato il nostro passato. Oggi, il *cyber*nauta (ovvero il navigatore della rete) può svolgere a distanza qualunque tipo di attività solitamente svolta fisicamente, in qualità di lavoratore, di consumatore, di paziente sanitario e, nell'ultimo anno e mezzo, anche di studente; a prescindere dalla sua esperienza nella navigazione, questi ha imparato a servirsi dei mezzi informatici affiancando - ed in alcuni casi anche sostituendo - alla sua identità reale una identità digitale (facilmente modificabile) che gli consente di utilizzare ogni possibile servizio digitale, dalle videochiamate al VPN[1] per le aziende, dal BYOD[2] alle piattaforme di *networking*[3] e didattica a distanza. Tali servizi caratterizzano ormai anche il rapporto con la Pubblica Amministrazione, relativamente alla quale il processo di digitalizzazione si è consolidato a partire dal 2005, anno in cui il Legislatore ha introdotto nel nostro ordinamento il Codice dell'Amministrazione digitale[4].

A fronte dell'esponenziale sviluppo delle tecnologie digitali e della continua globalizzazione delle reti di *computer* si registra, però, un aumento della criminalità informatica - ovvero della commissione di nuovi tipi di crimini/delitti informatici ma anche di crimini comuni realizzati grazie all'uso degli strumenti informatici[5] - che è,

[1] L'acronimo significa *Virtual Private Network* e rappresenta la rete virtuale privata nelle telecomunicazioni, instaurata come connessione tra soggetti che utilizzano, quale tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso - ad esempio i protocolli *Internet* - al fine di offrire alle aziende, ad un costo minore, le stesse possibilità offerte dalle linee private a noleggio, ma sfruttando reti condivise pubbliche.

[2] Acronimo che significa *Bring your own device*, ovvero "porta il tuo dispositivo". Il BYOD rappresenta una politica aziendale che consente di creare due ambienti diversi sullo stesso dispositivo, con dati aziendali e dati personali (chiamate, SMS, localizzazione GPS) rigorosamente separati. In pratica, esso permette di portare i propri dispositivi personali nel posto di lavoro e di usarli avendo, contemporaneamente, la possibilità di usufruire degli accessi privilegiati alle informazioni aziendali e alle loro applicazioni; è usato anche in ambito educativo per gli studenti che utilizzano i loro dispositivi. Oltre a BYOD, si usano anche le espressioni BYOPC - "*bring your own personal computer*" -, BYOT – "*bring your own technology*" -, BYOP – "*bring your own phone*" che, invece, significano "porta il tuo pc, porta la tua tecnologia e porta il tuo telefono" e che rispondono alla stessa politica aziendale.

[3] Le piattaforme di *networking* sono "luoghi" in cui, in rete, gruppi di persone più o meno grandi sono connessi fra loro e dialogano.

[4] Istituito grazie al D. Lgs. 7 marzo 2005, n. 82 al fine di riunire ed organizzare le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese, il CAD ha subito, nel corso di questi sedici anni, varie modifiche ed integrazioni tutte accomunate dall'obiettivo della semplificazione, che rappresenta un traguardo che, purtroppo, non sembra ancora essere raggiunto dalla Pubblica Amministrazione del nostro Paese in cui, contrariamente agli ordinamenti di altri Paesi europei, si registra ancora un forte tasso di burocrazia e complessità che ostacola il conseguimento di risultati significativi in termini di sviluppo sostenibile e competitività del sistema Paese.

[5] Il tema degli attacchi informatici è molto indagato e studiato; *ex multis,* A. BONFANTI, *Attacchi cibernetici e* cyber war*: considerazioni di diritto internazionale*, in *Notizie di Politeia*, n. XXXIV vol. 132, 2018 pp. 118-127; R. BRIGHI,

purtroppo, inversamente proporzionale alla conoscenza che di essa si abbia, dato l'ingiustificabile ed ancora troppo elevato tasso di analfabetismo digitale derivante da una conoscenza molto basilare ed elementare sia degli strumenti che delle insidie che la rete può nascondere, con ripercussioni e conseguenze che, ormai, non possono essere più sottovalutate. Infatti, l'estensione generalizzata a chiunque dell'utilizzo della tecnologia, conseguente alla pandemia da Covid-19, ha fatto notevolmente e repentinamente aumentare le categorie di *cyber*nauti - purtroppo spesso improvvisati ed assolutamente ignoranti di sistemi *hardware* e *software* oltre che di sicurezza informatica – e con esse sono aumentati anche i problemi di gestione dei sistemi stessi, che hanno mostrato lacune, falle e vulnerabilità. In pratica, alla pandemia virale si è venuta ad affiancare la cd. "pandemia informatica" che ha fatto vacillare gli equilibri - evidentemente precari - e le strategie di *cybersecurity* sui quali si fondava un sistema solo apparentemente consolidato.

Sono, dunque, aumentate le condotte criminose come il *malware*[6], con il *phishing* ed il *ransomware*[7] - per citare quelle più pericolose - ma anche lo *spam*[8] o le *fake news*[9], in cui si può incorrere navigando in rete: tali condotte rappresentano, tutte, tecniche utilizzate per riuscire ad intaccare la sfera della *privacy* e del diritto all'informazione, determinando la ben più grave conseguenza del furto dell'identità digitale.

Il saggio si sofferma proprio sui più frequenti e noti attacchi criminali informatici - che costituiscono fattispecie penalmente rilevanti - evidenziandone peculiarità e caratteristiche che danno vita a problematiche inerenti la gestione e la tutela tanto dell'identità digitale quanto dei dati personali immessi in rete, con ripercussioni sul tema della tutela della *privacy* e della stessa attività della Pubblica Amministrazione che è particolarmente esposta al rischio di tali attacchi, divenendone spesso vittima.

In realtà, non dovrebbe essere così, in quanto la digitalizzazione dovrebbe servire all'amministrazione a riuscire a svolgere la propria attività in maniera semplificata ed improntata al principio della "buona amministrazione"; ciononostante, invece, è frequente che gli stessi strumenti grazie ai quali essa dovrebbe conseguire tali

---

Cybercrimine *e anonimato in Rete. Riflessioni su sicurezza, efficacia investigativa e tutela delle libertà personali*, in *Sicurezza e Scienze Sociali*, n. 3, 2017; M. PALMIRANI, M. MARTONI, Big data, governance *dei dati e nuove vulnerabilità*, in *Notizie di Politeia*, n. 136, 2019, pp. 9 – 22.

[6] Il termine *malware* nasce dalla combinazione di due parole, *malicious*, ovvero dannoso, e *software* e con esso si fa riferimento a *software* destinati molto probabilmente ad attività fraudolente, quali, ad esempio, i *trojan horse*, i *ransomware*, i *virus*, i *worm* e i *malware* bancari su cui ci si soffermerà nelle pagine seguenti. La loro natura insidiosa sta innanzitutto nella difficoltà di riconoscerli a prima vista, aspetto, questo, che rende particolarmente difficile riuscire a contrastarli.

[7] Per la trattazione approfondita si rinvia al paragrafo 4.

[8] Lo *spam* è un messaggio pubblicitario non richiesto che viene inviato ad un numero molto elevato di utenti di *Internet* tramite posta elettronica.

[9] Le *fake news* sono le notizie false, o anche le *pseudo* notizie, che vengono diffuse attraverso i mezzi di informazione grazie ad articoli o pubblicazioni che contengono informazioni inventate, ingannevoli o distorte, divulgate al mero scopo di creare disinformazione o anche scandalo. Ovviamente sono fortemente favorite dall'utilizzo dei mezzi di comunicazione di massa, in particolare i *social media*.

ISSN 2036-7821

risultati diventino quelli che mettono in pericolo i suoi sistemi informatici e, dunque, i dati e l'attività che essa gestisce - come è accaduto assai di frequente anche ed in particolare nel periodo della recente pandemia.
Ci si soffermerà, dunque, sulle possibili cause di questi fenomeni, ed in particolare sulla scarsa alfabetizzazione digitale (diffusa non solo tra i singoli utenti individuali ma anche all'interno delle pubbliche amministrazioni, il cui personale non è preparato a sufficienza su questi temi) e sulla frammentarietà e poca incisività della normativa, a livello nazionale quanto europeo, che solo di recente sembra essersi finalmente orientata verso la realizzazione di una necessaria azione congiunta da parte di tutti gli attori politici, attraverso il Reg. (UE) 2021/887 istitutivo del Centro Europeo di competenza per la cybersicurezza e la Legge 109/2021 istitutiva dell'Agenzia per la *cyber*sicurezza nazionale in Italia.

2. Digitalizzazione e cybersecurity.
Specificamente nell'ambito dell'attività della Pubblica Amministrazione, l'applicazione delle ICT (*Information and Communication Technologies*) ha portato alla nascita dell' *e-government* (amministrazione digitale, appunto[10]) che ha assunto un rilievo particolare, in quanto ha consentito quella semplificazione, amministrativa e normativa, che, nelle intenzioni del Legislatore, deve condurre ad una maggiore efficienza attraverso lo sviluppo di modalità di azione ed organizzazione orientate al più efficace perseguimento di finalità di interesse pubblico: in pratica, riorganizzare le relazioni interne al sistema pubblico per migliorarne l'efficienza e, quindi, la capacità di risposta alle domande dei cittadini attraverso l'uso delle tecnologie dell'informazione e della comunicazione[11].

[10] La letteratura in tema di amministrazione digitale è vastissima. Si tratta, infatti, di un tema che ha impegnato sin da subito la dottrina allo studio e all'indagine sull'impatto che le tecnologie informatiche avrebbero avuto in un settore così delicato, interrogandosi *in primis* su cosa abbia inteso il Legislatore del 2005 per "amministrazione digitale" e cosa lo abbia portato alla maturazione di un Codice *ad hoc*. Ovviamente, oggetto di indagine e di analisi sono stati sia il rapporto del CAD con le disposizioni in materia di accesso, di trasparenza, di *privacy*, sia la nascita, in capo ai cittadini ed alle imprese, nell'attuale società dell'informazione, di nuovi diritti, e cioè quelli all'uso delle tecnologie, i quali, «*configurati come pretese giuridicamente assistite, sono suscettibili di attivare un meccanismo virtuoso di "induzione" dell'innovazione amministrativa*». Cfr. E. CARLONI (a cura di), *Codice dell'Amministrazione Digitale. Commento al D.Lgs. 7 marzo 2005, n. 82*, Maggioli Editore, Rimini, 2005; ma si veda anche F. FERRARI, *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico,* in *Riv. Dir. Proc. Civ., 2007; ed ancora* E. CARLONI, *Amministrazione aperta e* governance *dell'Italia digitale*, in Giornale dir. amm., 2012, 11, 1041; Id., *L'amministrazione aperta, Regole e limiti dell'*open Government, Maggioli editore, Rimini, 2014; Id., *Tendenze recenti e nuovi principi della digitalizzazione pubblica,* in *Giorn. Dir. Amm.*, 2015, 2; G. DUNI, *L'Amministrazione digitale*, Giuffrè, Milano, 2008; G. PESCE, *Amministrazione digitale: genesi, sviluppi, prospettive,* Editoriale Scientifica, Napoli, 2018; *Rivista di diritto dei media,* 2/2018R. CAVALLO PERIN e D. U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale,* Giappichelli, Torino, 2020.

[11] Tale il contenuto della Comunicazione del 26 settembre 2003 della Commissione Europea che ha descritto l'*e-government* come il processo di informatizzazione della Pubblica Amministrazione che si realizza attraverso «*l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche*

ISSN 2036-7821

Questa è la ragione per la quale digitalizzazione e semplificazione sono stati gli obiettivi perseguiti dal Legislatore anche in altre disposizioni normative[12] successive all'introduzione del CAD, e per la quale, nel tempo, la nozione di *e-government* si è profondamente evoluta, al passo con il progresso delle ICT, che costituiscono un settore nel quale i cambiamenti sono costanti e molto rapidi e richiedono che anche il metodo tradizionale di elaborazione scientifica ed ermeneutica sia connotato da una certa elasticità, mobilità e flessibilità[13].

Nel 2016 la Commissione Europea ha adottato la Comunicazione COM(2016)/179[14] con la quale ha fissato i principi di base cui deve ispirarsi l'azione per l'*e-government* relativa al periodo 2016-2020[15], richiedendo, in particolare, che l'azione di implementazione delle nuove tecnologie nel settore dell'*a*gere amministrativo tenda e si ispiri ai valori della massima trasparenza, efficienza ed inclusività affinché vengano erogati «*servizi pubblici end-to end senza frontiere, il più possibile personalizzati ed intuitivi a tutti i cittadini e a tutte le imprese nell'UE*». Lo strumento necessario e funzionale alla realizzazione di questi obiettivi è stato rinvenuto nel principio del libero accesso ai dati ed ai servizi delle amministrazioni pubbliche, sia a livello nazionale che transfrontaliero, grazie al quale realizzare un effettivo coinvolgimento delle parti nel processo decisionale ed una maggiore responsabilizzazione delle pubbliche amministrazioni, in un'ottica di crescita e di competitività[16].

Gli indubbi vantaggi che il processo di digitalizzazione dell'amministrazione pubblica ha determinato e può arrecare in prospettiva si scontrano, però, con le difficoltà applicative che una disciplina così articolata può incontrare nel contesto reale dell'attività istituzionale delle autorità pubbliche, connotato, purtroppo, da forti squilibri che sono la conseguenza inevitabile non solo di risorse insufficienti e, spesso, di grande arretratezza infrastrutturale e tecnologica, ma anche di complessità burocratiche. In pratica, la Pubblica Amministrazione non appare attrezzata, innanzitutto per l'incompetenza specifica dei funzionari; a tale aspetto si aggiunge il c.d. *digital divide*, ovvero il divario digitale che, nella popolazione, si registra fra coloro che conoscono ed utilizzano efficacemente gli strumenti informatici e coloro

---

organizzative ed all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici ed i processi democratici e di rafforzare il sostegno alle politiche pubbliche».

[12] Basti pensare, ad esempio, al decreto legge n. 5/2012, convertito con modificazioni dalla legge n. 35/2012, recante "Disposizioni urgenti in materia di semplificazione e di sviluppo" fino ai più recenti decreto Semplificazioni, D.L. n. 76/2020, convertito nella L. 120/2020 e decreto Semplificazioni *bis*, ovvero il D.L. 31 maggio 2021, n. 77 convertito nella L. 29 luglio 2021, n. 108.

[13] E. CARLONI, *La semplificazione telematica e l'Agenda digitale*, in *Giornale di diritto amministrativo* 7/2012, pp. 708-714.

[14] Del 19.4.2016.

[15] hiip://ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-179-IT-F1-1.PDF.

[16] Cfr. F. MARTINES, *La digitalizzazione della pubblica amministrazione*, in *Rivista di diritto dei media* 2/2018, 2.

ISSN 2036-7821

che, invece, per varie ragioni, non se ne servono[17]. Tutto ciò crea un inevitabile rallentamento del nostro Paese rispetto ai tempi funzionali alle politiche di *e-government*, specie se lo si paragona ad altri Paesi UE che sono molto più evoluti da questo punto di vista.

In ragione di quanto evidenziato, l'azione di promozione della digitalizzazione della Pubblica Amministrazione può porre rilevanti problemi in termini di sicurezza dei dati da essa raccolti, gestiti e custoditi e che possono facilmente essere esposti al rischio di attacchi informatici perpetrati in rete.

Si è resa, dunque, necessaria la nascita di una vera e propria disciplina deputata alla prevenzione ed alla cura delle patologie che il *web* contrae, e cioè delle minacce informatiche, che rappresentano «*qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone*»[18]: tale disciplina è la *cybersecurity* (sicurezza informatica) che, invece, rappresenta «*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*»[19].

Quando si parla di *cybersecurity* si fa riferimento al termine che, col tempo, si è venuto a sostituire a quelli più tecnici di *computer security* ed *information security*: inizialmente, la sicurezza era orientata a garantire il funzionamento delle reti pubbliche di comunicazione (a partire, in particolare, dalla Direttiva 90/387/CE sull'istituzione del mercato interno per i servizi delle telecomunicazioni); successivamente, però, si è giunti ad una nuova visione, incentrata sulla protezione dei dati e delle informazioni nella strategia europea del *Digital Single Market*, all'interno della quale la sicurezza dell'informazione è divenuta un pilastro per creare un clima di fiducia nell'ambiente digitale. Attualmente, dunque, con tale termine si fa riferimento proprio alla capacità di difendere e proteggere il *cyber*spazio dalla minaccia cibernetica, all'interno di un perimetro che non è solo relativo ad una dimensione spaziale di sicurezza nazionale e sovranazionale, ma che fa riferimento anche a nuovi valori, che esistono perché esiste la rete e che sono fatti di dati,

[17] Su questo aspetto rilevano particolarmente sia il dato anagrafico della popolazione italiana - che, per oltre il 50%, è rappresentata da persone che si sono formate in un'epoca in cui l'accesso alla tecnologia non era diffuso quanto lo è oggi – sia l'evidenza che i programmi di studio ministeriali delle scuole dell'obbligo ancora oggi prevedono una formazione sulle materie informatiche assolutamente inadeguata rispetto al progresso nel settore delle ICT registrato nell'ultimo ventennio. Cfr. F. MARTINES, *La digitalizzazione della pubblica amministrazione,* cit.

[18] Art. 2, punto 8) del già citato Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 19 aprile 2019 relativo all'ENISA, l'Agenzia europea per la *cyber*sicurezza e alla certificazione della *cyber*sicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).

[19] Art. 2, punto 1) del citato Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA.

ISSN 2036-7821

informazioni, diritti costituzionalmente protetti, che anche la pandemia da Covid-19 ha messo seriamente a rischio[20].

La *cybersecurity*, insomma, è necessaria proprio per l'acquisita consapevolezza che la tutela da minacce informatiche ormai involge strettamente il funzionamento di istituzioni e comunità e determina l'esigenza di affrontare la questione attraverso un quadro legislativo più articolato e complesso, nazionale quanto europeo, al fine di fornire ai clienti/cittadini protezione e tutela adeguate, uniformi e affidabili.

Per proteggere i sistemi, infatti, non basta che le Pubbliche Amministrazioni (o anche le imprese) sappiano individuare gli attacchi di cd. *spear phishing* (ovvero di *phishing* mirato); è necessario anche che esse siano dotate degli strumenti che consentano di prevenirli, proteggendo in maniera adeguata i propri sistemi attraverso politiche puntuali che diano vita ad azioni mirate.

Ma è, altresì, necessario che sia superato il generalizzato analfabetismo digitale, partendo innanzitutto dagli utenti individuali, che sono quelli che immettono in rete il maggior numero di dati, spesso in maniera inconsapevole, ed ai quali è, pertanto, necessario garantire una maggiore sicurezza, attraverso, *in primis*, una adeguata informazione, sia sui rischi che sugli strumenti di tutela, partendo innanzitutto dalla identità digitale di ciascuno, strumento al tempo stesso sensibile ed essenziale per accedere al mondo virtuale, ma di cui si ignora troppo facilmente l'importanza e che, pertanto, viene sottovalutato.

3. L'identità digitale e la sua tutela giuridica.

Il primo passaggio da compiere è, dunque, chiarire cosa sia l'identità digitale.

Ciascun individuo possiede una propria identità che lo connota all'interno della società, distinguendolo dagli altri consociati[21]; essa altro non è che il complesso delle risultanze anagrafiche che, a sua volta, rappresenta il risultato di un processo di

[20] Si ritiene, insomma, che a fronte di quanto evidenziato, il contenuto della *cybersecurity* si sia talmente dilatato ed evoluto da potere essere essa considerata un "bene pubblico" Cfr., al riguardo, R. BRIGHI e P. G. CHIARA, *La* cybersecurity *come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* in federalismi.it, n. 21/2021, pp. 25 e ss.

[21] Questa è la definizione che la Suprema Corte di Cassazione ha dato delle identità nella sentenza n. 978 del 1996, individuandola come «*il complesso delle risultanze anagrafiche, che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici ed a distinguerlo dagli altri consociati*». In realtà, l'attività giurisprudenziale sul diritto all'identità personale era stata molto intensa già a partire dalla metà degli anni Settanta del secolo scorso, quando, per la prima volta, con la sent. Pret. Roma 6.5.74, *GI,* I, 2, 514, essa viene riconosciuta come nuovo diritto. Circa dieci anni dopo, la Suprema Corte di Cassazione ha confermato tale riconoscimento con la sentenza del cd. caso Veronesi (sent. n. 3769 del 22.6.1985, *FI,* 1985, I, 2211) ed il tema è stato oggetto non solo di altre sentenze della stessa Corte di Cassazione, ma anche della Corte Costituzionale (ad es. sent. n. 13/1994, *GiurCost.* ,1994, 95; ma anche n. 297/1996, *GiurCost,* 1996, 2475). Esso nasce come promanazione del diritto all'immagine e si concretizza, sostanzialmente, nell'interesse di ciascun individuo a «*non vedere travisato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, professionale, a causa dell'attribuzione di idee opinioni o comportamenti differenti da quelli che l'interessato ritenga propri e abbia manifestato nella vita di relazione*», cfr. G. PINO, *L'identità personale,* in AA.VV., *Gli interessi protetti nella responsabilità civile*, vol. II, Utet, Torino, 2005, pp. 367- 394.

ISSN 2036-7821

identificazione plasmato dal contesto sociale in cui si sviluppa, dal diritto che la governa e dalle esperienze e convinzioni personali. Per tali motivazioni, l'identità personale rientra tra i beni giuridici tutelati dall'ordinamento che, attraverso tale tutela, protegge l'interesse del soggetto ad essere rappresentato nel contesto sociale in cui vive ed in cui esprime la sua personalità, in modo da potere mantenere il proprio onore, il decoro, la reputazione, l'immagine e, al contempo, avere riconosciuto un generale diritto di controllare la propria rappresentazione all'interno della società.

L'avvento delle nuove tecnologie e il progressivo e massiccio affermarsi della digitalizzazione hanno reso necessaria la nascita, al fianco dell'identità personale, dell'identità digitale che, invece, costituisce «*la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale*[22]» secondo le modalità previste dal Legislatore: in pratica, essa è un insieme di dati che vengono raccolti, memorizzati e condivisi digitalmente all'interno di un ecosistema di attori e che consentono di identificare univocamente una persona, un'azienda o un oggetto che, grazie alla propria identità, possono accedere ai servizi digitali.

Come previsto dall'art. 9 della "Dichiarazione dei diritti in *Internet*", l'identità digitale è il diritto ad avere una rappresentazione integrale e aggiornata delle proprie identità in rete, da definire e costruire liberamente sulla base dei dati che si sceglie di fornire e che sono, poi, quelli strettamente necessari ad adempiere agli obblighi previsti dalla legge, per la fornitura di beni e servizi e per l'accesso alle piattaforme che operano in *Internet*[23].

Il documento in questione è stato elaborato, nel 2015[24], dalla Commissione per i diritti e i doveri relativi ad *Internet* proprio a questo fine, ovvero per conferire un

[22] Tale è la definizione che ne ha dato, all'art. 1, comma 1, lett. o), il Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014, meglio noto come decreto SPID, recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese". Come si chiarirà meglio in seguito, lo SPID (Sistema Pubblico di Identità Digitale) è uno strumento di notevole semplificazione burocratica attraverso cui le pubbliche amministrazioni possono fornire l'accesso ai propri servizi; di esso, però, non sembra essersi ancora dotata tutta la popolazione, nonostante ne sia stata prevista l'obbligatorietà a partire dal 28 febbraio 2021. Cfr. A. F. SPAGNUOLO, E. SORRENTINO, *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, su *Federalismi.it*, n. 8/2021, pp. 274 – 287.

[23] Tale norma è intitolata "Diritto all'identità" e recita: «1. *Ogni persona ha diritto alla rappresentazione integrale e aggiornata delle proprie identità in Rete. 2. La definizione dell'identità riguarda la libera costruzione della personalità e non può essere sottratta all'intervento e alla conoscenza dell'interessato. 3. L'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano. 4. Ogni persona ha diritto di fornire solo i dati strettamente necessari per l'adempimento di obblighi previsti dalla legge, per la fornitura di beni e servizi, per l'accesso alle piattaforme che operano in Internet. 5. L'attribuzione e la gestione dell'Identità digitale da parte delle Istituzioni Pubbliche devono essere accompagnate da adeguate garanzie, in particolare in termini di sicurezza*».

[24] Esattamente il 14 luglio 2015.

fondamento costituzionale a principi e diritti maturati in uno spazio - quello di *Internet*, appunto - all'interno del quale andavano strutturati i rapporti tra le persone e tra queste e le istituzioni, sia dal punto di vista pubblico che da quello privato[25]. In tale spazio la suddetta Dichiarazione ha voluto che fossero riconosciute la libertà, l'uguaglianza, la dignità e la diversità di ogni persona, al fine di garantire il funzionamento democratico delle istituzioni e di consentire che *Internet* rappresenti il luogo in cui le persone e i gruppi possano autorganizzarsi ed in cui siano promosse l'eguaglianza sostanziale e la partecipazione individuale e collettiva ai processi democratici[26]. Pertanto, essa riconosce e disciplina innanzitutto il diritto di accesso a tale spazio - da intendersi, ovviamente, come accesso sostanziale e non come mera possibilità di collegamento alla rete - che deve essere garantito «*in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale*»[27] e, soprattutto, in modo che i propri dati trasmessi e ricevuti in *Internet* siano tutelati e non subiscano discriminazioni o restrizioni di alcun tipo[28].
La Dichiarazione, inoltre, consente che gli utenti possiedano molteplici identità digitali ed anche che mantengano l'anonimato nella rete.
Alla libera scelta dell'utente di fornire e gestire i propri dati corrisponde, poi, l'attività delle istituzioni pubbliche che, nel momento in cui attribuiscono l'identità digitale, devono adeguatamente garantirla e tutelarla, soprattutto in termini di sicurezza rispetto ai pericoli derivanti dall'aumento dell'utilizzo di *Internet* e dall'evoluzione degli strumenti tecnologici che consentono la diffusione e la condivisione dei dati personali *on line*.
Insomma, dal punto di vista giuridico, sono stati predisposti gli strumenti che consentono di esercitare liberamente il proprio diritto a possedere un'identità digitale quale mezzo di interazione umana e di sviluppo della personalità nel contesto messo a disposizione dalla rete. Tale identità appare necessaria fino al punto da risultare equivalente a quella personale, perché grazie ad essa «*il "patrimonio umano digitale" si fraziona in chiave d'accesso ad un patrimonio materiale (bancomat, carte di credito, ecc.), strumenti per un guadagno commerciale (il valore economico dei dati personali in sé), domicilio virtuale, estrinsecazione della proprietà intellettuale e strumento per i rapporti sociali* (on line)*: una proiezione complessa, economicamente più appetibile e più facilmente riproducibile dell'identità personale*[29]».

[25] Si tratta di un documento che consta di quattordici articoli.
[26] Dal *Preambolo* alla Dichiarazione dei diritti in Internet.
[27] Art. 2 commi 2 e 3.
[28] Artt. 4, 5 e 6.
[29] G. MALGIERI, *Il furto di "identità digitale": Una tutela "patrimoniale" della personalità,* in Atti del convegno "Giustizia penale nella rete", Diplap e Università di Perugia del 19.11.2014.

ISSN 2036-7821

Nel nostro ordinamento la disciplina sull'identità virtuale è contenuta nel Codice dell'Amministrazione Digitale[30] che, dal 2005 ad oggi, ha subito modifiche finalizzate a renderlo sempre più uno strumento di consolidamento del processo di digitalizzazione che ha investito la Pubblica Amministrazione, (oltre che la società in genere)[31]. Le più recenti tra queste, e cioè quelle contenute nel cd. Decreto Semplificazioni del 2020[32], hanno ulteriormente inciso sulla disciplina in esso contenuta, introducendo misure di semplificazione per il sostegno e la diffusione dell'amministrazione digitale[33], perfezionando e semplificando proprio l'istituto dell'identità digitale, oltre che quello del domicilio digitale e dell'accesso ai servizi digitali[34].

Tale ultimo intervento normativo ha confermato la consapevolezza, da parte del Legislatore, della necessità - ormai fortemente avvertita - che l'identità digitale sia "autentica[35]", ovvero che sia strettamente legata a quella reale, diversamente da

[30] Specificamente all'art. 3 *bis* che prevede «*Chiunque ha il diritto di accedere ai servizi* on-line *offerti dai soggetti di cui all'articolo 2, comma 2, lettere a) e b), tramite la propria identità digitale*».

[31] Si fa riferimento, specificamente, alle integrazioni contenute nel D.P.R. 12 aprile 2006, n. 184 che, all'art. 13, ha disciplinato l'accesso per via telematica ai documenti; ma anche alle modifiche contenute nella L. 17 dicembre 2012, n. 221 (conversione, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese) che, tra le misure urgenti di crescita del Paese, annoverava l'Agenda e l'identità digitale, i dati di tipo aperto, l'Agenda digitale per l'istruzione, la sanità digitale, ma puntava anche all'azzeramento del divario digitale ed al maggiore utilizzo della moneta elettronica. Successivamente a tale legge ci sono stati il D. Lgs. 22 agosto 2016 n. 179 (emanato in attuazione della legge delega n. 124/2015 di riforma della P.A. e finalizzato a definire un quadro normativo idoneo ad abilitare e supportare le azioni di attuazione dell'agenda digitale) e il D. Lgs. 13 dicembre 2017 n. 217 (finalizzato, invece, alla promozione della cittadinanza digitale – cfr. al riguardo, M. CAPORALE, *Dalle* smart cities *alla cittadinanza digitale*, su federalismi.it, 2/2020, pp. 30-47). *Ex multis*, G. CASSANO, C. GIURDANELLA (a cura di), *Il codice della Pubblica Amministrazione Digitale Commentario al D.lgs. n. 82 del 7 marzo 2005*, Milano, Giuffrè Editore, 2008; C. GIURDANELLA, *Il nuovo codice dell'amministrazione digitale (CAD)*, in *diritto.it.* 2017.

[32] D.L. 76/2020, conv. in L. 120/2020.

[33] Segnatamente, il Decreto Semplificazioni ha dedicato il suo Titolo III alle "Misure di semplificazione per il sostegno e la diffusione dell'amministrazione digitale" e, in particolare, si vedano gli artt. da 24 a 32.

[34] In ragione di tali ultime modifiche, dalla data del 28 febbraio 2021 le uniche credenziali tramite le quali si può accedere ai servizi digitali della Pubblica Amministrazione sono l'identità digitale SPID (Sistema Pubblico di Identità Digitale) e la Carta d'identità elettronica italiana (CIE). Si tratta di due strumenti digitali con il valore di un qualsiasi documento d'identità che saranno utilizzati nello svolgimento di pratiche amministrative *on line*, e che consentiranno anche transazioni elettroniche, con procedure semplificate e, soprattutto, sicure. Saranno utilizzati da tutte le amministrazioni - dallo Stato agli enti territoriali e locali, agli enti pubblici in genere - e renderanno possibile eliminare completamente le molteplici varie credenziali che, ancora oggi, sono necessarie per accedere ai servizi pubblici digitali, con un duplice vantaggio, uno per i cittadini ed uno per la Pubblica Amministrazione. I primi, infatti, non dovranno più ricorrere a credenziali diverse a seconda del servizio che vogliono usare; le seconde, invece, non dovranno farsi carico di gestire sistemi di rilascio e gestione delle credenziali di accesso dei propri utenti, con un evidente risparmio di risorse e di tempo. A partire da tale data, in pratica, sussisterà un unico sistema di identificazione digitale dei cittadini, grazie al quale produrre autocertificazioni, utilizzare applicazioni, effettuare pagamenti e ricevere notifiche digitali da varie agenzie pubbliche.

[35] L'identità digitale "autentica" è quella che è stata sottoposta ad un processo, appunto, di autenticazione, grazie al quale provare e garantire che essa corrisponda a chi ne attesta l'attribuzione a sé. L'autenticazione può realizzarsi attraverso "un solo fattore" - ovvero facendo ricorso ad una *username* e ad una *password* – ed attraverso

ISSN 2036-7821

quanto accadeva in passato, quando, cioè, una stessa persona poteva tanto dotarsi di un'identità digitale anonima, quanto averne molteplici.
Oggi, invece, anche rispetto all'identità digitale prevale il requisito della trasparenza e, pur costituendo, questa, lo strumento di accesso ad un mondo - quello virtuale - in cui non si deve necessariamente essere visibili, è, tuttavia, importante che le due forme di identità coincidano, al fine di garantire una migliore sicurezza sul *web* e di apprestare una maggiore difesa contro gli attacchi informatici finalizzati a violare la *privacy* e la libertà.
Oltre che essere presente nel CAD, il concetto di "identità digitale" è stato introdotto anche nel codice penale – mediante il D.L. n. 93/2014[36] - e precisamente al comma terzo dell'art. 640-*ter*, attraverso il quale è punita la fattispecie criminosa della frode informatica con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.
Con tale norma il Legislatore ha, per la prima volta, riconosciuto che costituisca reato il procurare «*a sé o ad altri un ingiusto profitto con altrui danno, mediante alterazione in qualsiasi modo del funzionamento di un sistema informatico o telematico o intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti*». Se, poi, il fatto viene commesso mediante il furto o l'indebito utilizzo dell'identità digitale in danno di uno o più soggetti, è previsto un aumento di pena[37].
Una disposizione, quella in questione, che si è resa necessaria per tutelare l'identità digitale dai notevoli e maggiori rischi cui è esposta e che derivano proprio dal fatto che essa nasce e si muove all'interno dello spazio virtuale, in cui è molto più semplice accedere a dati ed informazioni che si trovano in rete grazie all'evoluzione degli strumenti tecnologici che ne consentono la diffusione e la condivisione, e che spesso non sono protetti adeguatamente. Diventa, allora, più semplice il fenomeno del c.d. "*identity theft*" - ovvero del furto di identità digitale - favorito sia dalla possibilità di creare agevolmente degli *account* falsi da parte di soggetti terzi, sia dalle erronee modalità di custodia delle credenziali da parte degli utenti che, a causa della scarsa preparazione e conoscenza degli strumenti che hanno a disposizione, possono cadere vittime di azioni specificamente finalizzate al furto di tali credenziali oppure dirette ad ottenere informazioni e dati di natura personale da utilizzare per l'accesso a sistemi informatici sostituendosi alla vittima.

4. *Il preoccupante fenomeno del "furto di identità digitale".*

"più fattori" – ovvero avvalendosi di una chiave fisica di sicurezza, una tessera magnetica o una *smart card* legata ad una *password*, a cui possono aggiungersi anche informazioni biometriche come l'iride o l'impronta digitale o vocale, ad esempio.

[36] Convertito con modificazioni dalla L. 15 ottobre 2013 n. 119.

[37] Infatti, la reclusione aumenta da due a sei anni e la multa può variare da 600 euro a 3000 euro.

ISSN 2036-7821

Dunque, il mondo virtuale favorisce delle grandi opportunità ma determina anche dei seri problemi: in contrapposizione ai vantaggi ed alla semplicità di accesso ad esso consentita ai *cyber*nauti esistono insidie che vanno necessariamente conosciute per potere essere evitate o superate.

Una di queste è il furto d'identità digitale[38] (c.d. "*Identity Theft*") che rappresenta un preoccupante fenomeno in continua espansione proprio perché correlato all'uso ormai generalizzato di *Internet*[39].

Pur non trattandosi "materialmente" di una sostituzione di persona, tale fattispecie è stata equiparata, nel nostro ordinamento, al reato disciplinato dall'art. 494 c.p.[40] (appunto quello relativo alla sostituzione di persona), norma che, in realtà, era stata introdotta per punire condotte operanti nel mondo analogico e secondo modalità e stratagemmi ben lontani da quelli che il mondo digitale ha reso, poi, possibili. Infatti, nelle iniziali intenzioni del Legislatore, essa faceva riferimento alla commissione di azioni relative alla "falsità personale" e alla "fede pubblica" quale bene giuridico tutelato dalla norma e identificato nella «*fiducia che la società impone negli oggetti, segni e forme esteriori ai quali l'ordinamento attribuisce un valore importante*»[41].

La dimensione digitale della nostra epoca ha, però, implicato una necessaria evoluzione non solo della tipizzazione di questo reato, ma anche del bene giuridico da proteggere e, dunque, il reato di furto di identità digitale (anch'esso a tutela della fede pubblica, plurioffensivo, a forma vincolata e fondato su un'attività ingannatoria) si configura come furto realizzato tramite, ad esempio, i c.d. "*fake*" dei *social network*, il *phishing* o le innumerevoli altre falsificazioni di identità realizzate per condotte abusive; mentre il bene giuridico da proteggere ad esso relativo è, appunto, l'identità digitale.

Specificamente, la sua "plurioffensività" deriva dal fatto che esso lede contemporaneamente più interessi protetti *ex lege*, sia di natura pubblica – e, dunque, appartenenti alla collettività – che di natura privata – e, cioè, destinati ad incidere e a produrre effetti nella sfera giuridica del singolo individuo. Mentre il suo essere "a forma vincolata" richiede che esso sia commesso soltanto in una delle modalità

[38] Interessanti sono, al riguardo, gli scritti di B. PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, 2020; A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di Diritto penale* – Cybercrime, Wolters Kluwer, 2019; F. DI TANO, R. BRIGHI, *Identità, anonimato e condotte antisociali in rete. Riflessioni informatico-giuridiche*, in *Rivista di filosofia del diritto*, 2019, fasc. 1, pp. 183-204; C. CRESCIOLI, *La tutela dell'identità digitale*, in *Diritto Penale Contemporaneo*, 5/18; C. PECORELLA, *Reati informatici*, in *Enc. Dir.* X 2017, p. 722; F. CORONA, *La nascita dell'identità digitale e conseguenze*, in AA VV, Stalking, *atti persecutori*, cyber*bullismo e tutela dell'oblio*, IPSOA, 2017.

[39] C. CAVACEPPI, F. S. CAVACEPPI, D. CAVALLARO, R. COLETTI, A. CONTALDO, A. CORTESE, *La responsabilità nei nuovi reati informatici – Mezzi di ricerca e acquisizione della prova*, Maggioli Editore, 2020.

[40] Tale norma recita «*Chiunque, al fine di procurare a sé o ad altri un ingiusto vantaggio o di recare ad altri un danno, induce taluno in errore sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino ad un anno*».

[41] Lavori Preparatori al codice penale, II, m. 490, 242.

ISSN 2036-7821

espressamente previste ai sensi di legge (vale a dire nei casi in cui un soggetto sostituisca illegittimamente la propria all'altrui persona, oppure attribuisca a sé o ad altri un falso nome, un falso stato o una qualità da cui possano derivare effetti giuridici) e che non sia configurabile in forma omissiva.

Sotto il profilo soggettivo si realizza una condotta - perseguibile d'ufficio - con dolo specifico, in quanto l'autore agisce con la coscienza e la volontà di compiere il fatto e con la finalità ulteriore di arrecare un danno alla vittima o un vantaggio a se stesso[42] - di natura tanto patrimoniale quanto non patrimoniale[43] - non rilevando che il vantaggio sia effettivamente ottenuto o il danno realmente arrecato, ma essendo sufficienti la volontà di perseguire tale fine e l'inganno della fede pubblica. Infatti, la Suprema Corte di Cassazione ha sostenuto che, rispetto a tale reato, sia giuridicamente configurabile anche la forma del tentativo: da ciò deriva che il reato non è perseguibile solo se sia stato consumato e si sia verificata l'induzione in errore del soggetto passivo, ma anche se l'agente si sia limitato ad usare uno dei mezzi fraudolenti previsti *ex* art. 494 c.p., ma non sia, tuttavia, riuscito ad indurre in errore taluno[44].

La Suprema Corte si è più volte pronunciata sulle attività di falsificazione virtuali, concludendo che «*la condotta di colui che crea ed utilizza un* account *di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete con lo scopo di arrecare un danno al soggetto le cui generalità siano state abusivamente spese, integra il reato di cui all'art. 494 c.p.*»[45]. In buona sostanza, essa ha affermato che la condotta del soggetto che crea ed utilizza *account* o caselle di posta elettronica servendosi di dati anagrafici di un terzo soggetto che non ne è consapevole può indurre in errore non solo il fornitore del servizio, ma l'intera generalità degli utenti, ignari del fatto di stare interagendo con una persona diversa da quella che credono sia realmente. In tal modo si integra la fattispecie prevista dall'art. 494 c.p.[46], perché ai delitti contro la fede pubblica deve riconoscersi, oltre che

---

[42] Va rilevato che la Cassazione ha ritenuto che, nel novero dei vantaggi, rientri "*il nuovo bene immateriale per antonomasia, rappresentato dalla visibilità, che può dar luogo – ad esempio – alla creazione di falsi profili di personaggi famosi, al solo scopo di attrarre a sé l'attenzione di numerosi contatti che, altrimenti, non avrebbero mai fatto parte della rete sociale dell'autore*» (Cass. pen., 16.6.2014, n. 25774). In particolare, per la Suprema Corte la vanità rappresenta perfettamente la finalità indicata dalla norma; dunque, il reato si configura, ad esempio, quando ci si crea una falsa identità su un *social network* per soddisfare una propria "velleità narcisistica" che rappresenta un vantaggio non patrimoniale, mentre il danno alla vittima è costituito dalla lesione all'immagine e alla dignità della stessa. Cfr. M. MARRAFFINO, *Sostituzione di persona mediante furto di identità digitale,* in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale - Cybercrime*, UTET Giuridica, 2019, p. 316.

[43] M. MARRAFFINO, *Sostituzione di persona mediante furto di identità digitale,* cit., 307-330.

[44] Cfr. Cass. pen., 6.1.2015, n. 8278. Siccome, dunque, non è necessario riuscire a realizzare compiutamente la condotta, ma è sufficiente avere tentato di indurre in errore la vittima attraverso atti idonei e non equivoci diretti alla realizzazione della stessa, il reato si configura anche se la vittima si accorge tempestivamente della sostituzione e "blocca" il contatto.

[45] A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale - Cybercrime*, cit.

[46] Cass. pen., 8.11.2007, n. 46674.

ISSN 2036-7821

un'offesa alla fiducia che la collettività ripone in determinati atti, simboli o documenti, anche un'ulteriore e potenziale attitudine offensiva, che può rivelarsi, poi, concreta in presenza di determinati presupposti, avuto riguardo alla reale e diretta incidenza del falso sulla sfera giuridica di un soggetto[47].

Il reato di sostituzione di persona è stato ritenuto, inoltre, integrabile sia nei casi in cui si finga di essere una persona di sesso diverso da quello reale, sia nei casi in cui ci si attribuisca una inesistente qualifica professionale - creando, ad esempio, una falsa identità su *Skype* o sui *social network* - grazie alla quale invitare a colloqui fittizi vittime ignare quando, in realtà, lo scopo è solo quello di corteggiarle o di aumentare i propri *follower* o contatti.

Per la Corte di Cassazione, infatti, «*oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p., è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia di un determinato destinatario, così il Legislatore ha ravvisato in essi una costante insidia alla fede pubblica e non soltanto alla fede privata e alla tutela civilistica del diritto al nome*[48]».

Sebbene sia cospicua la giurisprudenza sul reato di sostituzione di persona commesso a mezzo *Internet*, va rilevato che, purtroppo, il tema presenta delle inevitabili zone oscure (all'interno delle quali si affievolisce la stessa percezione dell'offensività del fatto) determinate dalla difficoltà di riuscire realmente ad identificare l'utente che crea un falso profilo e dalla frequenza con cui il *cyber*nauta si interfaccia con false identità (nonostante, ad esempio, i *social network*, all'interno delle condizioni che fanno sottoscrivere agli utenti, vietino espressamente di farvi ricorso).

In ogni caso, la norma dell'art. 494 c.p. ha consentito di stigmatizzare una condotta in cui si può facilmente e frequentemente cadere, ed è stato possibile che essa fosse estesa ai reati commessi nel mondo virtuale perché, ormai, le relazioni virtuali hanno assunto la stessa portata di quelle reali, anche in sede civile, ed è giusto che pure rispetto ad esse siano tutelate la fede pubblica e la fiducia dell'utente nelle condotte altrui[49].

Al contempo, però, va detto che, nonostante abbia consentito, e consenta tuttora, di sanzionare una pluralità di fattispecie in perfetta sincronia con il progresso delle tecnologie, la formulazione generica di tale norma non può essere completamente

[47] Cass. SS. UU., 25.11.2007, n. 46982. I giudici hanno punito anche la condotta realizzata con finalità "ludica" o vendicativa, condannando un soggetto che, partecipando con un nickname ad una chat di carattere erotico, aveva fornito agli altri utenti il numero di cellulare della sua ex datrice di lavoro anziché il proprio, come forma di vendetta nei suoi confronti a causa di una controversia civilistica che aveva in corso con lei. La conseguenza di tale condotta era stata che quest'ultima, vittima ignara, si era trovata a ricevere telefonate e messaggi SMS, anche in ore notturne, da parte di uomini che la credevano disponibile ad incontri di natura sessuale. Cfr. Cass. pen. 28.11.2012, n. 18826. A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale - Cybercrime*, cit.

[48] Cass. pen., sez. V, 14.12.2007, n. 46674.

[49] A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale - Cybercrime*, cit.

ISSN 2036-7821

sufficiente per una figura così complessa e specifica come quella del furto di identità digitale.

Il profilo digitale di una persona è cosa ben diversa da quello reale e materiale della stessa[50], e se il furto di un'identità digitale (magari attraverso la sottrazione delle credenziali di accesso agli *account*) può risultare semplice per chi realizza tale condotta approfittando, spesso, della scarsa capacità della vittima di rendersene conto, gli effetti che derivano a quest'ultima sono molteplici e nient'affatto "statici", perché possono estendersi e coinvolgere tutti gli aspetti della sua sfera soggettiva, lasciandola esposta a conseguenze seriamente dannose nel lungo periodo e che non si limitano al solo evento della pura sostituzione di persona.

Sarebbe, invero, necessario creare una norma *ad hoc,* che commisuri il trattamento sanzionatorio in relazione alla reale ed effettiva portata degli effetti che da tale reato si producono nella sfera giuridica dell'individuo che lo subisce.

Ma se è vero che il Legislatore deve pensare ad una disciplina più appropriata e che sanzioni più specificamente la condotta in esame, è altrettanto vero che, come si è già avuto più volte modo di sottolineare, anche l'utente debba imparare a tutelarsi da solo, in via preventiva, non solo informandosi, ma anche compiendo gesti come, ad esempio, il frequente cambio delle *password*, il non divulgarle, il non ripeterle per tutte le attività digitali che compie, operazioni che, pur nella loro semplicità e banalità, gli consentirebbero di predisporre una prima basilare forma di difesa della propria identità da tutte quelle attività criminose – come quelle di *spear phishing* – che possono condurre al furto di essa[51].

---

[50] M. C. GAETA, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi*, in *Dir. informaz. e informatica*, fasc. 1, 1.2.2018, 147 ss.

[51] Quando si accede abusivamente ad un sistema informatico - quale una piattaforma *social* o un'*app* di messaggistica istantanea - rubando l'identità di un soggetto, la vittima non sarà solo costui (il quale, tra l'altro, può anche ignorare del tutto che siano state rubate le sue credenziali) ma anche coloro che, a qualunque titolo, siano destinatari delle attività che, grazie a tale furto, vengono realizzate, e che possono tanto limitarsi al "semplice" scambio epistolare utilizzando le *app* di messaggistica, spacciandosi per il titolare dell'identità, quanto estendersi ad attività di natura illecita, quali frodi commerciali o acquisti *on line*. Ecco perché, accanto al reato disciplinato dall'art. 494 c.p., è altrettanto pericoloso incorrere in quello di "accesso abusivo a sistema informatico" disciplinato dall'art. 615-*ter* c.p. Tale norma è stata introdotta nel codice penale dall'art. 4 della l. 23 dicembre 1993, n. 547 e prevede che «*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*». Essa è posta tra i delitti contro l'inviolabilità del domicilio (art. 614 c.p.) di cui condivide sia la funzione sociale che il trattamento sanzionatorio, prendendo in considerazione due condotte: quella dell'accesso non autorizzato (abusivo) ad un sistema informatico e quella dell'illecito mantenimento. Come quello disciplinato dall'art. 494 c.p., anche il reato di accesso abusivo a sistema informatico è plurioffensivo; ma per esso, il bene giuridico tutelato dalla norma è l'inviolabilità del domicilio informatico, anche più della violazione del diritto alla riservatezza. Sia la giurisprudenza che la dottrina ritengono che per tale fattispecie non debbano essere adottate o predisposte particolari misure di sicurezza, in quanto è necessario che il titolare abbia la volontà di reprimere qualsiasi irruzione nel suo sistema con accorgimenti tecnici, informatici e logici. Pertanto, il reato si perfezionerà anche se viene violata una sola delle misure di sicurezza predisposte dal titolare. Cfr. F. S. CAVACEPPI, *Attacchi intrusivi e distruttivi di sistemi informatici,* in F. PELUSO (a cura di) *La responsabilità nei nuovi reati informatici,* Maggioli, 2020, 142.

5. Lo spear phishing *ed il* social engineering, vulnera *ai sistemi informatici.*

Come detto, dunque, il livello elevato di analfabetismo digitale impedisce una corretta e adeguata conoscenza di cosa rappresenti realmente la digitalizzazione e, quindi, del mondo virtuale; i *cyber*nauti si accontentano spesso di un approccio molto basilare, quello strettamente necessario e funzionale alla navigazione, senza porsi affatto il problema delle conseguenze e dei rischi in cui si possano imbattere "avventurandosi" in rete in maniera incauta ed inconsapevole. Si comprende bene, dunque, che l'ignoranza possa avere ripercussioni sia per il singolo individuo che per altri soggetti e posizioni, in quanto la potenzialità *nocendi* di certe condotte non resta circoscritta.

I rischi più frequenti in cui si può incorrere sono senz'altro gli attacchi di *spear phishing*, che rappresentano una delle insidie più pericolose che la navigazione in rete può nascondere, perché puntano alla buona fede ed alla inconsapevolezza degli utenti, di cui ci si approfitta per impossessarsi di dati importanti allo scopo di riutilizzarli in maniere molteplici[52].

Tramite lo *spear phishing*, in pratica, vengono realizzate truffe che sono contenute all'interno di comunicazioni elettroniche o *e-mail* indirizzate a persone, organizzazioni o aziende specifiche, sia pubbliche che private, e che sono messe in atto con l'obiettivo di sottrarre dati per fini dannosi, ma anche allo scopo di installare *malware* (ovvero *software* malevoli) sul *computer* dell'utente preso di mira. Sono dei veri e propri attacchi intrusivi e distruttivi di sistemi informatici che, spesso, vengono erroneamente definiti attacchi *hacker*[53], con i quali, invece, non vanno confusi.

Infatti, l'*hacking* è quell'attività attinente al funzionamento di un sistema informatico ed alle misure di sicurezza poste a sua protezione, svolta per lo più dagli amministratori del sistema stesso attraverso un «*insieme di tecniche ed operazioni volte a conoscere, accedere e modificare un sistema informatico* (hardware *o* software)»[54]. Il termine *hacker* che da esso deriva, dunque, indica colui che pratica l'attività di *hacking* e che ha come obiettivo quello di acquisire un'accurata padronanza del sistema su cui interviene per adattarlo alle sue esigenze in maniera del tutto lecita - ad esempio, per incrementare alcune prestazioni *hardware* o, ancora, per rimuovere limitazioni al funzionamento di componenti elettronici o di applicazioni o, al contrario, per aggiungere funzioni ad un programma.

---

[52] Si tratta di attacchi di *phishing* mirato, che, cioè, hanno come bersaglio una sola persona e che si differenziano dagli attacchi di *spray phishing* che, al contrario, sono attacchi di massa, in cui si cerca di coinvolgere quante più vittime possibile.

[53] Termine che deriva da *hacking*, sostantivo che fa riferimento alla pirateria informatica.

[54] F. S. CAVACEPPI, *Attacchi intrusivi e distruttivi di sistemi informatici*, cit., 129.

ISSN 2036-7821

L'attività di *hacking* realizzata dall'*hacker* diventa attività di *cracking* - realizzata, invece, dal *cracker*[55] - quando i metodi e le tecniche lecite del primo vengono utilizzati per aggirare l'acquisto delle licenze e per accedere ai sistemi altrui con lo scopo di impadronirsi dei dati riservati e di danneggiarne il funzionamento. Questo tipo di condotta, evidentemente, non è lecito perché il *cracker*, analizzando le risposte che il *software* fornisce a determinati *input*, riesce a comprenderne il funzionamento al fine di violarlo[56].

La tecnica che più facilmente egli utilizza è quella del *social engineering* (ovvero del raggiro tramite l'inganno) perché è quella grazie alla quale egli riesce a realizzare e distribuire *software* in violazione del *copyright* che li protegge, in tal modo superando e scapolando l'unico e vero ostacolo che si frappone al tentativo di violare il sistema dall'esterno, e cioè l'evoluzione del *software* stesso.

In pratica, nascondendo la propria identità e sfruttando l'inesperienza e la buona fede delle vittime, i criminali informatici riescono a ricavare da un sistema informazioni che altrimenti non potrebbero ottenere.

Il "contenitore" - o veicolo - preferito e più facile da utilizzare per realizzare tali truffe è, da vari anni a questa parte, proprio quello dei *social network* che, essendo utilizzati da chiunque, rappresentano non solo il luogo dal quale trarre ogni tipo di informazione, ma anche quello tramite cui orientare ed influenzare le masse e su cui fare circolare notizie anche false e tendenziose - le *fake news* - a cui si è portati a credere a prescindere da un eventuale controllo di corrispondenza al vero e di scientificità e che, grazie alla condivisione e alla pubblicazione che i *social* consentono, si divulgano rapidamente, determinando, spesso, il risultato di destabilizzare un determinato ordine pubblico e di mettere in pericolo la sicurezza informatica degli stessi utenti.

Essendone questa la *ratio*, si comprende facilmente, dunque, perché quelli attuati tramite attacchi di ingegneria sociale sono dei veri e propri reati informatici: e cioè perché la condotta illecita si realizza sui sistemi informatici, infettandone i programmi e i dispositivi al fine di attuare molestie, estorsioni o ricatti tramite dei *software* intrusivi e malefici (i *malware*) sotto forma di *virus* informatici (i quali, a loro volta, sono caratterizzati dalla peculiarità di essere "contagiosi"), ma anche di *Trojan Horse*, *Ransomware*, *Spyware*[57] e *Malvertising*[58], per citarne alcuni[59]. Ognuna di tali

[55] Il significato di tale termine, infatti, è *rompere, spezzare,* ma anche *decifrare.*

[56] Questa modalità è nota come *reverse engineering* e consiste nell'analizzare i programmi e cercare di capirne il funzionamento in assenza del codice sorgente che appartiene alla casa sviluppatrice. Il risultato che ne deriva non è lecito quando le risposte del *software* a determinati *input* vengono analizzate al fine di riuscire a violare il sistema.

[57] Si tratta di *software* che vengono installati su di un sistema per raccogliere informazioni da trasmettere ad un destinatario interessato e che possono riguardare tanto le abitudini di navigazione, quanto le *password* o le chiavi crittografiche di un utente.

ISSN 2036-7821

tipologie ha la sua potenzialità *nocendi*, per potersi difendere dalla quale è importante innanzitutto saperla individuare e, dunque, conoscere.
Specificamente, infatti, i *virus* sono dei *software* (quindi programmi o codici) realizzati al fine di compromettere o di manipolare il funzionamento di un sistema informatico, allo scopo, ad esempio, di arrecarvi spreco di risorse o distruzione di dati. Attraverso un programma che ne consente la progettazione tramite un linguaggio molto semplice, essi sono in grado di trasformare il *software* in *malware* (*malicious software*)[60], e cioè in programma malevolo.
La loro contagiosità deriva dal fatto che essi si auto-replicano, ovvero creano copie di se stessi all'interno di altri *file* o *computer* senza il consenso o l'intervento di un utente: qui essi vivono un periodo di incubazione durante il quale restano latenti, senza compiere alcuna attività apparente; al termine di tale periodo, infettano alcuni elementi strategici *hardware* e *software* del *computer* e, quando le condizioni prestabilite dagli algoritmi di programmazione si realizzano, si propagano ed iniziano ad infettare sia *file* della stessa macchina che *file* appartenenti a dispositivi esterni ad essa, fino a che non vengano riconosciuti ed estirpati.
I *file* all'interno dei quali i *virus* si diffondono non sono malevoli, ma, ciononostante, essi diventano un tramite per l'infezione grazie a frammenti di *software* parassiti che si inseriscono nei codici eseguibili già esistenti, agendo contro le necessità dell'utente per rubargli informazioni sensibili: dunque, la loro pericolosità è direttamente proporzionale alla quantità e alla riservatezza dei dati presenti sul disco.
La minaccia contenuta nei *Trojan Horse*, invece, si diffonde con lo stesso "effetto sorpresa" determinato dal ben noto cavallo di Troia, apparentemente dono benevolo ma, nei fatti, contenitore di uomini nascosti che, riusciti ad entrare, tramite esso, nella città, la distrussero, approfittando della buona fede di quegli stessi abitanti che avevano fatto entrare il cavallo perché non si aspettavano alcuna insidia o trappola. Allo stesso modo, i *trojan* possiedono le sembianze di un *software* innocuo, ma al loro interno contengono un'insidia che viene diffusa grazie alla inconsapevole complicità della vittima designata che, inviandolo, contribuisce a realizzare l'attacco.

---

[58] Termine che deriva dalla sintesi delle parole m*alicious* e *advertising*, e che fa riferimento agli attacchi che originano dalle pubblicità delle pagine *web*.

[59] Oltre a quelli citati, ci sono anche i *rabbit*, gli *adware*, i *file batch*, i *backdoor*, i *dialer*, i *keylogger*. Un altro genere di minacce che "viaggia" attraverso il *web* è lo *skimming*, attraverso il quale "si inietta" un codice (*script*) malevolo in siti che vendono beni e servizi anche attraverso *malvertising*, compromettendo l'infrastruttura utilizzata per gli annunci pubblicitari, con l'obiettivo di carpire le informazioni sensibili dei clienti.

[60] La possibilità – matematicamente dimostrata da Von Neumann - di realizzare programmi in grado di riprodurre delle copie del proprio codice in maniera autonoma risale, in realtà, già al 1949. Invece, nei primi anni Settanta, un ingegnere che lavorava in una società che contribuì a sviluppare le reti per lo scambio di pacchetti dati usati nel programma ARPANET - Bob Thomas – ideò un *malware*, denominato *Creeper*, che è considerato il primo *worm* della storia, ovvero il primo *malware* in grado di autoreplicarsi e di diffondersi in altri dispositivi. Infatti, il nome *creeper* deriva dalla scritta che compariva sui *monitor* dei pc infettati: *I'M THE CREEPER: CATCH ME IF YOU CAN*. S. CAVACEPPI, *Attacchi intrusivi e distruttivi di sistemi informatici*, cit., 131.

ISSN 2036-7821

Quest'ultimo, dunque, non è reso possibile dall'auto-replicazione come accade per i *virus*, bensì dall'invio del *software* che stesso l'utente provvede a fare, ingannato dalle funzionalità "lecite" ed utili che esso apparentemente manifesta ma che, invece, nascondono istruzioni dannose e che vengono eseguite all'insaputa dell'utilizzatore.
Diversamente dai *Trojan Horse*, i *Ransomware*, invece, attuano un vero e proprio ricatto che può risolversi (in teoria) solo pagando un riscatto. Si tratta di *malware* che criptano tutti i dati presenti su un disco secondo una chiave di cifratura complessa, per riuscire a crittografare la quale l'unica soluzione è pagare il riscatto richiesto dal *cracker* che, tramite essi, ha infettato il *computer*.
Proprio perché si attua una vera e propria richiesta di riscatto, il *ransomware* è un reato che rientra a pieno titolo nel delitto di estorsione disciplinato dall'art. 629 del codice penale[61], con la differenza, rispetto a questo, che il primo si realizza a livello telematico, attraverso la prospettazione di una ingiustizia futura, dipendente dalla volontà dell'agente, che può essere inviata grazie ad una *e-mail*, ai *social network*, ma anche grazie ad icone che compaiono sullo schermo e che si inseriscono nel sistema informatico. Una volta che vi si siano inseriti, il sistema è infettato ed i *file* in esso contenuti e memorizzati sul disco (dai documenti, alle immagini, ai *file* personali) vengono criptati e resi irrecuperabili, al punto da risultare compromesso lo stesso funzionamento del sistema.
Terminata questa fase, sullo schermo compare un avviso di avvenuta infezione con la richiesta di riscatto di una somma di danaro che dovrà essere corrisposta entro i termini perentori indicati, se si vuole ottenere la chiave che consente il recupero dei propri *file*. La vittima designata, proprio perché è stata messa nell'impossibilità di utilizzare il suo sistema e non vuole, ovviamente, perdere i propri dati, a questo punto cede al ricatto, preferendo pagare l'importo che le viene richiesto (che, solitamente, non è molto elevato) e che è l'unica condizione per riuscire ad ottenere l'invio della *mail* contenente il programma di decriptazione[62].
Purtroppo, però, il pagamento del riscatto non è sempre risolutivo, in quanto può non avere impedito che i dati rubati siano stati già duplicati (e che siano, dunque, rimasti nelle mani del criminale) o che, magari, essi siano stati cancellati, con un conseguenziale e potenziale danno di notevole entità[63] che può riguardare gli utenti

[61] Tale norma recita «*Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000*».

[62] Di solito il pagamento del riscatto avviene tramite *Bitcoin* o comunque attraverso mezzi non tracciabili, e questo aspetto rende complicato individuare il luogo ed il momento di effettivo conseguimento del profitto.

[63] Riguardo ai *ransomware*, va evidenziato che la Suprema Corte di Cassazione penale, con la sent. n. 2728 del 18 novembre 2011 (in www.penale.it), ha affermato che nell'espressione "cancellazione" di dati (tipologia di reato configurata dall'art. 635 *bis* c.p.) non si fa riferimento ad una "irrecuperabile elisione", in quanto essa comprende anche la rimozione provvisoria dei dati, rimediabile con un successivo intervento recuperatorio. In pratica, la Suprema Corte ha voluto evidenziare che il danneggiamento informatico dei dati si verifica solo quando l'attacco abbia comportato una perdita definitiva dei dati stessi. Si considera, invece, commessa la *cyber* estorsione,

ISSN 2036-7821

comuni, ma anche le aziende, le infrastrutture informatiche strategiche e le pubbliche amministrazioni (enti pubblici, ospedali o servizi pubblici in genere). La peculiarità del *ransomware*, infatti, è proprio quella di propagarsi rapidamente attraverso la ricerca dei collegamenti in rete, cifrando e rendendo non fruibili i dati memorizzati che, a loro volta, rendono spesso inutilizzabili gli stessi sistemi, non solo quelli sui quali si sferra l'attacco, ma anche il *server* centrale, i sistemi collegati, i dispositivi di *back-up*, le cartelle condivise da altri utenti: insomma, non è compromesso solo il singolo operatore, ma anche l'intero ufficio o l'ente stesso[64], ledendo ed offendendo, in tal modo, interessi e beni giuridici connessi alle tecnologie dell'informazione, come la *privacy* e la sicurezza informatica, la libertà e la confidenzialità delle comunicazioni[65].

Alla categoria dei *ransomware* - la cui nocività appare evidente - appartengono i più noti programmi utilizzati per compromettere l'integrità, la disponibilità e la riservatezza dei dati e dei sistemi informatici[66]; essi sono in grado di realizzare condotte molteplici, non solo di danno effettivo ma anche di pericolo di danno[67], ormai riconosciute e punite come reati grazie alle previsioni contenute nella Convenzione di Budapest sulla criminalità informatica[68].

Tale atto è stato emanato dal Consiglio d'Europa il 23 novembre 2001 con il precipuo obiettivo di realizzare una politica comune tra gli Stati membri attraverso l'adozione di una legislazione appropriata e adeguata a combattere il *cybercrime* in maniera coordinata tra i vari Paesi aderenti. Essa rappresenta il primo Accordo internazionale sui crimini commessi attraverso *Internet* o altre reti informatiche ed è stata ratificata da sessantacinque Paesi, compresa l'Italia, che tramite la legge di ratifica n. 48 del 18

---

cumulativamente e non alternativamente, con violenza e minaccia e, dunque, si configura la violenza informatica, nei casi in cui il *malware* abbia compromesso solo il funzionamento del sistema, ad esempio disattivando le opzioni di avvio o bloccando l'intero schermo. Cfr. F. CAVACEPPI, *Attacchi intrusivi e distruttivi di sistemi informatici,* cit. 139.

[64] Tra gli attacchi a mezzo *ransomware* più rappresentativi a livello globale si segnalano quelli del 2016 *all'Hollywood Presbiterian Medical Center* e quello al sistema di trasporto pubblico di San Francisco, come evidenziato dal Rapporto *Clusit* del 2017, ovvero il rapporto annuale elaborato dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT, appunto) che promuove attività relative alla sicurezza informatica, costituendo un luogo privilegiato di scambio di esperienze ed informazioni.

[65] Dal punto di vista della tipologia di reato, dunque, il *ransomware* può individuarsi come reato comune, il cui soggetto attivo può essere chiunque ed il cui soggetto passivo può essere anche un soggetto ulteriore e diverso da quello che è titolare del rapporto giuridico e che, come conseguenza dell'attività illecita, subisce il danno al patrimonio. Infatti, è possibile che la minaccia di *ransomware* sia percepita sullo schermo del sistema aziendale di un dipendente o di un dirigente di una determinata azienda il quale, però, non è il diretto titolare del patrimonio attaccato, ma si limita solo ad utilizzarlo e, dunque, la minaccia si propaga a tutto il sistema aziendale.

[66] Specificamente essi sono *Cryptolocker, Cryptowall, Tesla, TorrentLocker, Wannacry, Cerber* e *Locky.*

[67] Tale è la condotta disciplinata dall'art. 615 *quinquies.* V. nota 71.

[68] Si fa riferimento all'art. 6 della Convenzione. Interessante, al riguardo, S. CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia Informatica e diritto*, in *Informatica e diritto.* XLI annata, Vol. XXIV, 2015, n. 1-2, Edizioni Scientifiche Italiane, pp. 153-164.

marzo 2008[69] ha introdotto importanti modifiche sulle specifiche tipologie di reati sia all'interno del Codice penale e del Codice di procedura penale[70], sia all'interno del Decreto sulla responsabilità amministrativa delle persone giuridiche[71] e del Codice in materia di protezione dei dati personali[72].

Il ruolo che la Convenzione di Budapest riveste attualmente è molto importante sul tema, non solo perché, ad oggi, essa rappresenta l'unico Trattato internazionale sul *cybercrime* e le prove elettroniche, ma anche perché, nel definire i reati informatici, fornisce gli strumenti per acquisire tali prove necessarie al fine di perseguirli nella giurisdizione di ciascun Paese aderente[73]. Inoltre, essa resta un atto assolutamente adeguato a criminalizzare anche condotte illecite non espressamente tipizzate e sanzionate (perché, magari, configuratesi successivamente alla sua emanazione), nonostante risalga a ben venti anni fa l'elenco specifico delle fattispecie di illeciti informatici da introdurre nella legislazione penale degli Stati che l'hanno ratificata. La sua versatilità è conseguenza del linguaggio tecnologicamente neutro e fluido in essa adoperato, grazie al quale i reati informatici descritti hanno potuto adattarsi facilmente a tutte le fattispecie criminose dell'ambito della cibernetica, estendendosi anche a quelle che sono venute ad esistenza successivamente al 2001, come conseguenza della notevole espansione della tecnologia, dell'informatica e della digitalizzazione.

Questo è quanto è accaduto, ad esempio, con il *phishing*, che rappresenta, attualmente, il fenomeno criminale più diffuso, e che, pur non essendo stato previsto né specificamente disciplinato originariamente dal Trattato di Budapest, ciononostante, ha potuto essere configurato tra i reati informatici grazie alla sua riconduzione a fattispecie come l'accesso abusivo a sistema informatico o la frode informatica, da esso disciplinate.

---

[69] Recante, appunto, "Ratifica della Convezione di Budapest sulla criminalità informatica".

[70] Si evidenzia che sia il codice penale che quello di procedura penale erano stati "aggiornati" in tema di criminalità informatica attraverso le modifiche e le integrazioni apportate dalla L. n. 547 del 23 dicembre 1993, con la quale erano state introdotte alcune norme che si occupassero specificamente della nuova tipologia di reati che il sempre maggiore utilizzo dell'informatica poteva determinare. La consapevolezza di dovere adottare condotte uniformi in materia, culminata nella Convenzione di Budapest, ha reso inevitabile modificare ulteriormente le stesse norme che la legge del 1993 aveva aggiunto agli impianti originari dei due codici, come è accaduto, ad esempio, con l'art. 615 *quinquies*, che disciplina e punisce la condotta di chi diffonde apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare o interrompere un sistema informatico o telematico. La fattispecie descritta in tale norma rappresenta un reato di pericolo; ciò significa che il Legislatore ha inteso conferire una particolare rilevanza a condotte che possano anche solo potenzialmente rappresentare una minaccia di danneggiamento e, dunque, non punisce solo l'effettivo verificarsi del danneggiamento o dell'interruzione, ma anche "semplicemente" la mera elaborazione di un sistema, un'apparecchiatura o un programma che siano di per sé idonei a creare il rischio di un danneggiamento.

[71] D. Lgs. n. 231/2001.

[72] Introdotto nel nostro ordinamento con il D. Lgs. 196 del 30 giugno 2003.

[73] Nella sua prima parte, relativa al diritto sostanziale, infatti, la Convenzione individua alcune condotte riconducibili al *cybercrime* indicandole come quelle da perseguire necessariamente; ad esse, ciascuno Stato può decidere di aggiungerne altre, anche ove non siano qualificate come condotte criminali in altri Stati.

ISSN 2036-7821

6. Il phishing e la sua disciplina come fattispecie delittuosa.

Il *phishing* è un'attività strettamente legata al furto dell'identità digitale; esso costituisce una delle minacce più pericolose in cui è attualmente possibile imbattersi navigando nel *web*, specie se non si è in grado di individuarle e, di conseguenza, di prevenirle[74].

La sua tecnica operativa di base[75] - che è una tecnica di *social engineering* - consiste nello sviluppo e nella creazione di un testo contenente un codice maligno (il *malware*, appunto) e che, sul piano dei contenuti, della struttura e della composizione grafica di riferimento, sia idoneo a determinare piena fiducia, rispetto al contenuto stesso, nel soggetto che lo riceve, inducendolo, per tale motivo, ad eseguire una specifica azione (ad esempio, attivare un *link* in ipertesto verso un sito *web* terzo). Il testo viaggia prevalentemente attraverso una *e-mail* che, oltre ad essere un vettore di infezione a livello globale, è anche più potente del *web* stesso, perché costituisce un canale di comunicazione preferenziale, normalmente utilizzato per condividere *file* sotto forma di allegati che, a loro volta, pure possono infettare, specie se sono creati, come spesso accade, con versioni obsolete e, quindi, facilmente aggredibili.

La *mail* è, pertanto, la tecnica più praticata per attuare la minaccia del *phishing*, oltre ad essere tra le più antiche e versatili per gli attacchi di *social engineering*: grazie ad essa si inducono gli utenti incauti a visitare un sito e ad inserire le proprie informazioni personali che saranno poi sottratte e sfruttate per commettere operazioni illecite, come il furto di dati personali, il furto di denaro o la compromissione delle reti aziendali[76].

Il termine *phishing* è una variante dell'inglese *fishing*, che significa "pescare", ed in effetti la funzione delle *mail* ingannevoli è esattamente la stessa degli ami e delle esche quando si va a pescare, vale a dire quella di fare abboccare gli utenti inconsapevoli allo stesso modo in cui si fanno abboccare i pesci[77]: in pratica, si invita

[74] Interessanti, in tema di *phishing*, R. FLOR, Phishing *e profili penali dell'attività illecita di "intermediazione" del cd.* financial manager, in *Diritto penale e processo*, 2012, 55-67; R. FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, n. 2-3, 2007; S. LOMBARDO, Phishing*: consigli utili per attenuare il rischio di adescamento*, in *Rivista ICT Security Collection*, n° 2, Ottobre 2018. Ma anche A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di Diritto penale* – Cybercrime, Wolters Kluwer, 2019, cit.

[75] Tale tecnica è detta *Deceptive Phishing*.

[76] Gli attacchi di *phishing*, dunque, si propagano attraverso un invio massivo ed indiscriminato di *mail* (cosiddetto *spamming*) da parte del soggetto attaccante, raggiungendo un numero indeterminato e casuale di persone.

[77] Sono note anche due ulteriori tipologie di *phishing*, e cioè lo *smishing* ed il *vishing*. Lo *smishing* (dalla combinazione delle parole SMS e *Phishing*) è il tentativo, da parte dei truffatori, di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS: in pratica, all'interno dell'SMS viene richiesto di fare *clic* su un *link* o di chiamare un numero di telefono per "verificare", "aggiornare" o "riattivare" l'*account* del destinatario. La truffa risiede nel fatto che tale *link* porta ad un sito *web* fasullo ed il numero di telefono conduce direttamente ad un truffatore che finge di essere la società legittima. Il *vishing*, invece, (dalla combinazione delle parole *Voice* e

ISSN 2036-7821

il destinatario, tramite l'invio di un'*e-mail*, a fornire dati riservati (come, ad esempio, il numero della propria carta di credito o la *password* di accesso al servizio di *home banking*[78], ma anche i dati di *login* agli *account* dei *social media*) sulla base di motivazioni di ordine tecnico cui questi è portato a credere in quanto la *mail* è contrassegnata dal logo di un istituto di credito o di una società di commercio elettronico che, in realtà, è contraffatto ma che, però, appare verosimile, per cui è credibile che da esso parta una richiesta come quella oggetto della *mail*[79]. Infatti, il mittente delle *e-mail* è, in linea generale, riconducibile, per contraffazione, ad enti pubblici, istituzioni e organizzazioni private la cui operatività e la cui presenza sono consolidate in un determinato ambito territoriale locale, nazionale o internazionale, anche rispetto al numero di persone ad essi fidelizzate. Una volta che tale contenuto abbia ingenerato nell'utente destinatario della *mail* la convinzione della necessarietà dell'attuazione della condotta che gli viene richiesta, la truffa si è realizzata ed il criminale informatico è riuscito a "pescare" una ingenua vittima che, semplicemente con un *clic*, navigando in rete e compiendo banalissime e comunissime attività, esegue quanto richiesto e rende possibile, inconsapevolmente, l'accesso ai suoi dati personali[80].

Phishing) è una truffa telefonica tramite la quale si cerca di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferire del denaro.

[78] L'*home banking* è la possibilità, per il cliente di una banca, di avere a disposizione servizi bancari grazie ai quali effettuare operazioni, mediante collegamento telematico e non necessariamente in presenza. Specificamente rispetto ad esso va segnalata un'importante pronuncia giurisprudenziale che ha lasciato, inevitabilmente, il segno in merito alla possibilità di tutelare il consumatore utente che cada vittima di un attacco *phishing*. Si fa riferimento alla sentenza n. 5895 del 2019 della II Sezione del Tribunale di Napoli, con la quale è stato condannato un istituto bancario, oltre che al pagamento delle spese e delle competenze legali al difensore degli attori, anche alla restituzione, in favore di questi, delle somme loro addebitate in qualità di vittime di frode perpetrata mediante *phishing*, in quanto «*nel rapporto contrattuale di* home-banking *la banca ha la veste di contraente qualificato, che, non ignaro delle modalità di frode mediante* phishing *da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza*». In pratica, tale pronuncia ha ribadito la necessità che la stessa cautela ed attenzione che vengono richieste al cliente quando compie le operazioni bancarie siano adottate dall'istituto bancario nel momento in cui le autorizza.

[79] Il soggetto passivo della *mail* è spinto ad eseguire l'azione proposta accedendo ad un sito *web* terzo, creato *ad hoc* dal *phisher* secondo i contenuti e gli schemi comunicativi tipici dell'ente, istituzione od organizzazione privata, della quale viene simulata la genuinità. A questo punto, la pagina *web* creata ad arte richiederà l'esecuzione di una specifica ed ulteriore azione da parte del soggetto passivo, quale, ad esempio, tra le più frequenti e comuni, l'inserimento di credenziali di accesso, di dati personali o di informazioni bancarie idonee a consentire al soggetto attivo della minaccia il conseguimento di un vantaggio economico effettivo, derivante dalla disponibilità e dal potenziale impiego delle informazioni illegittimamente acquisite.

[80] Particolarmente frequente è il rischio di cadere vittime di *phishing* rispetto al compimento di operazioni bancarie. In merito, la Corte di Cassazione, con l'ordinanza n. 9158 del 29 maggio 2018, ha stabilito che, al fine di garantire la fiducia degli utenti nella sicurezza del sistema, in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici «*è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo*». In pratica, alla banca è richiesta una diligenza di natura tecnica relativamente ai servizi di pagamento

ISSN 2036-7821

Giuridicamente il *phishing* costituisce un comportamento illecito proprio per questo, perché è finalizzato a rubare dati personali sensibili; solitamente esso inizia con la raccolta dei dati dell'utente per poi arrivare alla realizzazione di un evento materiale come la *deminutio patrimonii*[81] e la *iniusta locupletatio*[82], conseguenze di una condotta realizzata interamente *on line* e che pregiudica la sfera personale dell'individuo da parte di soggetti che riescono ad avvalersi di sistemi di mascheramento ed a restare "delocalizzati" grazie anche alla rapidità con cui la rete stessa consente l'esecuzione di tali sistemi.

Si tratta, dunque, di una fattispecie che trova i mezzi principali di esecuzione dell'attività fraudolenta nella condotta umana e nell'uso dello strumento informatico.

Il nostro ordinamento, però, non prevede uno specifico precetto penale rubricato come "*phishing*" e, dunque, come già accennato, la condotta delittuosa ad esso relativa viene fatta rientrare dalla giurisprudenza in fattispecie penali già disciplinate, tra le quali, oltre alla sostituzione di persona (art. 494 c.p.)[83], rientrano la falsificazione di comunicazione telematica (art. 617 *sexies* c.p.), la truffa (art. 640 c.p.[84]), l'accesso abusivo in un sistema informatico o telematico (art. 615 *ter* c.p.) e la frode informatica (art. 640 *ter* c.p.[85]). Tali fattispecie sono state, in gran parte, introdotte dal Legislatore nazionale già con la Legge n 547/1993, recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura

---

nel mercato interno (così come previsto dal D.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE) da valutarsi con il parametro dell'"accorto banchiere", e sarà, pertanto, attribuito ad essa l'onere della prova della riconducibilità dell'operazione al cliente.

[81] Diminuzione del patrimonio.

[82] Ingiustificato arricchimento.

[83] Va evidenziato, però, che, nella maggior parte dei casi, il mittente non si sostituisce ad una persona fisica, ma prevalentemente ad una persona giuridica (come una banca, le poste) e, dunque, non vi è la sostituzione tecnica all'altrui "persona".

[84] Tale norma disciplina il reato di "Truffa" che, in ordine alla tutela del patrimonio, punisce tutti quei comportamenti idonei ad alterare la libera formazione del consenso nei negozi giuridici patrimoniali attraverso artifizi o raggiri (che non siano manifestamente grossolani e non verosimili), indotti al fine di persuadere il soggetto passivo della bontà di una determinata scelta (così facendolo cadere in errore), anche con la minaccia di non incorrere in un danno maggiore. Ovviamente, lo scopo della condotta è riuscire ad ottenere un profitto ingiusto, con il relativo danno altrui, da intendersi come un vantaggio sostanzialmente economico. Il reato è istantaneo e si consuma con l'avvenuta diminuzione patrimoniale subita dalla persona offesa, a causa della condotta criminosa, ma è configurabile anche il tentativo. Il *phishing* può essere ricondotto al reato di truffa, in alcuni casi anche in concorso con il reato di cui all'art. 494 c.p. (sostituzione di persona). In ogni caso esso si configura nel momento in cui l'autore invia messaggi di posta elettronica solo apparentemente provenienti da mittenti "reali" e tale dato lo differenzia dalla truffa: infatti, mentre in quest'ultima l'elemento del danno deve avere necessariamente contenuto patrimoniale perché consiste in una lesione concreta e non soltanto potenziale, nella condotta del *phishing*, nel momento in cui si ottengono i dati di accesso della vittima, al *phisher* non deriva alcun vantaggio patrimoniale effettivo in danno di questa.

[85] Tale norma fa riferimento, invece, al reato di "Frode informatica", che riconduce a sé i comportamenti complessivi del *phishing*, e cioè l'alterazione del funzionamento di un sistema informatico e, in via alternativa o prodromica, l'intervento senza diritto su dati, informazioni o programmi contenuti nel sistema stesso, con il conseguimento dell'ingiusto profitto e dell'altrui danno.

ISSN 2036-7821

penale, in tema di criminalità informatica. Successivamente, esse sono state ulteriormente integrate a seguito dell'entrata in vigore della legge di ratifica della Convenzione di Budapest (la L. 18 marzo 2008, n. 48) grazie alla quale i *cyber crimes* - ai quali, appunto, appartiene la fattispecie del *phishing* – vengono identificati come «*ogni tipo di violazione penale commessa per mezzo, con l'ausilio e/o avente ad oggetto un sistema o programma informatico*».

Certamente, il fatto che la condotta del *phishing* sia non solo mutevole e realizzabile con differenti modalità, ma possa anche essere ricondotta a tante fattispecie delittuose rischia di non consentire di identificare quale sia il suo riferimento principale e, dunque, di non inquadrare stabilmente il fatto tipico in una disposizione normativa *ad hoc*. Anche per il *phishing*, infatti, ci si trova di fronte ad un'ipotesi di reato plurioffensiva, in quanto le condotte del *phisher* colpiscono differenti beni giuridici, e questo aspetto sembra portare all'unica conclusione che debba essere l'interprete a dovere applicare, volta per volta, le disposizioni che meglio valorizzano la specifica condotta criminosa, la quale sarà variabile sia rispetto all'effettivo danno causato sia rispetto alle variazioni della modalità operativa e tecnologica che, nello specifico caso, avranno caratterizzato il fatto criminoso.

In pratica, il giudice dovrà valutare quale delle condotte che integra il *phishing* nel singolo caso prevalga rispetto alle altre e, dunque, se vi sia un'ipotesi di concorso di reato tra la truffa e la sostituzione di persona rispetto alla diversa ed ulteriore fattispecie di accesso abusivo al sistema informatico ex art. 615 *ter* c.p. che, a sua volta, tutela il diverso bene giuridico del domicilio informatico. Se, però, prevalessero le condotte dell'accesso abusivo a sistema informatico (art. 615 *ter* c.p.) o della frode informatica (art. 640 *ter* c.p.) si finirebbe con il dovere escludere la responsabilità penale dell'intera fase di adescamento della vittima, valorizzata, invece, dai reati di truffa (art. 640 c.p.) o sostituzione di persona (art. 494 c.p.).

A fronte di tali considerazioni, resta, comunque, l'imprescindibile necessità di dovere fare riferimento ad un orientamento abbastanza costante, che la giurisprudenza prevalente ha individuato sussumendo la condotta del *phisher* in via principale all'interno del reato di frode informatica[86], in concorso formale di reato con l'eventuale ipotesi di accesso abusivo ad un sistema informatico[87].

7. La tutela delle identità virtuali nel Codice per la protezione dei dati personali.

[86] Aggravata dal comma III dell'art. 640 *ter* c.p.

[87] A seconda delle ipotesi, la giurisprudenza ha ritenuto che il *phishing* integrasse o la frode informatica e l'accesso abusivo, o la frode informatica e la detenzione o diffusione di codici o *password*. Recentemente, ha affermato che si configuri responsabilità penale per frode informatica (640 *ter*) anche nei casi di *phishing* effettuato mediante *e-mail* contenenti dati forniti direttamente (si veda Cass., II sez. penale, sent. n. 21987 del 14 gennaio 2019).

ISSN 2036-7821

La disciplina relativa agli attacchi informatici, ed in particolare al *phishing*, non può, però, essere costituita solo da norme che criminalizzano le condotte abusive ed involgono profili di sicurezza informatica, grazie alle quali proteggere l'identità dell'utente sotto il profilo dell'autenticazione e dell'identificazione informatica. Il bersaglio preferito di tali condotte, infatti, come evidenziato, è rappresentato dai dati degli individui, che sono oggetto di tutela sia se gestiti dal singolo individuo sia se gestiti dalla Pubblica Amministrazione[88], relativamente alla quale l'art. 50 del CAD stabilisce che «*i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati*».

In particolare, i dati personali sono definiti, dall'art. 4, comma 1, n. 1 del GDPR, come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*»[89], laddove la persona identificabile è «*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*». Nel merito, dunque, tra tali dati sono ricompresi tutti quelli che valgono a identificare la persona fisica, sia direttamente che a seguito di valutazione da parte dell'interprete in relazione a tutte le informazioni disponibili.

La Pubblica Amministrazione è titolare del potere di raccogliere, gestire, custodire ed anche pubblicare i dati che, in tale ultimo caso, sono qualificati come *open data*[90]; essa

[88] Sul tema della protezione dei dati la produzione scientifica è molto vasta; a titolo esemplificativo si citano G. CARULLO, *Dati, banche dati,* blockchain *e interoperabilità dei sistemi informatici nel settore pubblico,* in R. CAVALLO PERIN e D. U. GALETTA (a cura di) *Il diritto dell'amministrazione pubblica digitale,* Giappichelli editore, Torino, 2020, 191 - 217.; Id., *Big data e Pubblica Amministrazione nell'era delle banche dati interconnesse,* in *Concorrenza e mercato, 2016;* F. BALDUCCI – ROMANO, *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia,* in *Rivista italiana di diritto pubblico comunitario,* 2015; F. PIZZETTI, *La* privacy *come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona,* in P. BILANCIA, M. D'AMICO, (a cura di), *La nuova Europa dopo il Trattato di Lisbona,* Giuffrè, Milano, 2014; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*), in* Rivista di diritto internazionale, *2016, p. 690;*

[89] Sulla differenza tra dati e informazioni si rinvia, *ex multis,* a F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield), cit., 197 ss.; ma si vedano anche A. BONOMI, *Informazione e pubbliche amministrazioni. Dall' accesso ai documenti alla disponibilità delle informazioni,* Bari, Cacucci Editore, 2012; M. FALCONE, *Dati aperti e diritto al riutilizzo delle informazioni: la declinazione italiana del paradigma degli* open data, in B. PONTI (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni,* Rimini, 2016, p. 601 ss.; G. DE MINICO, Big data *e la debole resistenza delle categorie giuridiche.* Privacy *e* lex mercatoria, in *Dir. Pubb.*, 2019, 1, pp. 89-115

[90] Come previsto dall'art. 52, comma 2, del CAD che dispone che «*I dati e i. documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, […] si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 68, comma 3, del presente Codice, ad eccezione dei casi in cui la pubblicazione riguardi dati personali*». In tema di gestione dei dati, *ex multis,* V. BERLINGÒ, *Il fenomeno della* datafication *e la sua giuridicizzazione,* in Riv. trim. dir. pubbl., 2017, 641 ss.; ma

ISSN 2036-7821

deve, dunque, provvedere a conservarli in archivi digitali che, data la loro mole, devono consistere in strutture *ad hoc,* quali i cd. *cloud computing,* che rappresentano un modello economico innovativo improntato sull'offerta di beni e servizi personalizzati per l'innovazione e la digitalizzazione di tutti i settori. In pratica, essa delocalizza l'infrastruttura di memorizzazione dei dati affidandone il servizio di custodia a società esterne che professionalmente erogano questi servizi per conto di numerosi enti, sia pubblici che privati, e su tale attività di custodia dei dati effettua un necessario monitoraggio che, purtroppo, non sempre il personale interno alle amministrazioni è in grado di attuare in quanto, spesso, non possiede le competenze giuridiche e informatiche adeguate[91].

La gestione della molteplicità di dati da parte dell'amministrazione costituisce, dunque, una questione di non poco momento proprio per la facilità con cui essi possono essere sfruttati tramite le modalità di attacco informatico evidenziate, che partono dal cattivo uso che di essi si faccia per arrivare ad utilizzare - e, quindi, a compromettere - l'identità digitale stessa dell'utente.

Il Legislatore europeo ha dimostrato una notevole attenzione sul tema, per la necessità di apprestare la tutela più adeguata ai dati: infatti, con il recente Regolamento Generale sulla protezione dei dati[92] (GDPR - che, nel nostro ordinamento, è intervenuto a modificare il precedente Codice della *Privacy*[93]) ha previsto una serie di ulteriori garanzie e principi grazie ai quali poter mantenere il controllo sui dati immessi in rete, in particolare su quelli da cui possano emergere la personalità, le preferenze e, in generale, ogni informazione idonea a consentire a terzi la ricostruzione dell'identità personale di ciascun individuo.

Segnatamente, il GDPR prevede, all'art. 5, che i dati personali debbano essere trattati «*in modo lecito, corretto e trasparente nei confronti dell'interessato*» e che, dopo essere stati raccolti per finalità determinate, esplicite e legittime, debbano essere trattati secondo modalità che non siano incompatibili con tali finalità; anche la loro conservazione deve avvenire in maniera tale da consentire l'identificazione degli interessati «*per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*»; una conservazione per periodi più lunghi dovrebbe essere giustificata solo da fini di pubblico interesse, di ricerca scientifica o storica o a fini statistici, ed in ogni caso i

---

anche M. FALCONE, Big data *e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, Riv. trim. dir. pubbl., 2017, 601 ss.; F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla* privacy, in R. CAVALLO PERIN e D. U. GALETTA (a cura di) *Il diritto dell'amministrazione pubblica digitale,* Giappichelli editore, Torino, 2020, 43-79.

[91] F. MARTINES, *La digitalizzazione della pubblica Amministrazione,* cit. 9 ss.

[92] *General Data Protection Regulation* o GDPR, ovvero il Reg. UE 2016/679 che rappresenta la principale normativa europea in materia di protezione dei dati personali: esso è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018.

[93] D. Lgs. 196/2003; dopo l'entrata in vigore del GDPR il Codice per la *Privacy* ha subito le modifiche contenute nel D.lgs. 10 agosto 2018, n. 101 (attuativo del GDPR) e nella L. 27 dicembre 2019, n. 160.

ISSN 2036-7821

dati devono essere trattati «*in maniera da garantire un'adeguata sicurezza* […] *compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*». Grazie a tale norma l'interessato vede garantita non solo l'informazione circa le finalità, le modalità, la base giuridica del trattamento e il tempo di conservazione dei dati prima che venga effettuato qualunque trattamento, ma anche la conseguenziale possibilità di controllare la loro diffusione. Tale disciplina si completa con quella relativa al consenso (contenuta nel successivo art. 6) *condicio sine qua non* per la liceità del trattamento stesso e che l'interessato al trattamento dei dati deve necessariamente fornire, soprattutto quando dal trattamento dei dati non autorizzati possa derivare la ricostruzione di un profilo dell'utente idoneo ad incidere sulla sua libera determinazione come individuo nella società (particolarmente delicati risultano, in questo senso, i dati relativi alla salute o a precedenti penali).

Specificamente rispetto alla commissione delle condotte criminali che conseguono agli attacchi alla sicurezza informatica, il Codice contiene gli artt. 167 – relativo al Trattamento illecito di dati; l'art. 167 *bis* – relativo alla Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala; e l'art. 167 *ter* – relativo all'Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala. Tali norme sono tutte legate al concetto di identità digitale introdotto dall'art. 9 del D.L. 14.8.2013, n. 93 - convertito dalla L. 15.10.2013, n. 119 - che ha inserito nell'art. 640-*ter* c.p. l'aggravante per l'ipotesi in cui il fatto sia commesso «*con furto o indebito utilizzo dell'identità digitale*».

Come lo stesso GDPR ha richiesto, è necessario che vengano predisposte misure di sicurezza adeguate allo scopo di tutelare l'identità digitale; esso considera tali, al comma 2 dell'art. 32[94], innanzitutto quelle aventi l'obiettivo di rendere meno attaccabili i *database*, unica condizione possibile per tentare di ridurre i casi di sostituzioni di persona e accessi abusivi in generale. Tale norma, infatti, prevede espressamente che «*Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*». Nonostante tale previsione, però, gli attacchi informatici rendono possibile e attuabile il reato di sostituzione di persona in concorso con l'accesso abusivo a un sistema informatico in tutti i casi in cui il soggetto attivo riesca a forzare le credenziali di accesso della parte offesa, avendo, poi, la possibilità di eseguire operazioni per suo conto e realizzando,

[94] Rubricato "Sicurezza del trattamento".

ISSN 2036-7821

dunque, una sostituzione di persona con modalità esecutive diverse perché legate ai mezzi informatici[95].

Come ulteriore forma di tutela il Regolamento UE in questione ha, inoltre, rafforzato il diritto dell'utente di chiedere e ottenere l'accesso a tutti i propri dati personali con un'istanza da formulare direttamente al *provider*, così come potrà chiedere la cancellazione e il blocco di falsi *account* e di dati - fotografie incluse - condivisi illecitamente da eventuali *fake*.

In caso di mancata risposta o di risposta insufficiente a tale richiesta, questi potrà presentare un reclamo al Garante per la protezione dei dati personali, sì da ottenere l'accesso ai propri dati ed eventualmente il blocco immediato di quelli trattati illecitamente.

Il reclamo al Garante è un rimedio di tipo amministrativo consentito agli utenti *cyber*nauti che siano divenuti, loro malgrado, vittime di attacchi informatici a seguito dei quali sia stata loro rubata l'identità e, magari, creato un profilo *fake* dal quale partono i contenuti oggetto dell'estorsione[96].

Rispetto a tali casi, un ruolo essenziale è svolto dal Responsabile del trattamento dei dati personali, il quale deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che il trattamento dei dati in esame realizzi una tutela efficace e completa degli interessati, in particolare del loro diritto al rispetto della vita privata.

L'esercizio dell'azione amministrativa, comunque, non preclude quello dell'azione penale, che potrà e dovrà in ogni caso proseguire[97].

---

[95] Il reato può concretizzarsi anche più semplicemente nel caso in cui l'utente menta sulla propria età. Questo aspetto è stato oggetto di particolare attenzione da parte del Legislatore, in quanto da esso dipende la tutela del minore. Pertanto, è stato previsto che per potersi iscrivere ai *social network* e, in generale, ai servizi della società dell'informazione, bisogna avere compiuto l'età minima di 16 anni, che gli Stati Membri possono abbassare ulteriormente fino a 13 anni se lo ritengono opportuno, ed in tali casi sarà necessario provare il consenso prestato dall'esercente la responsabilità genitoriale (art. 8 GDPR). In Italia l'età per il consenso è stata fissata a 14 anni, anche per esigenze di coordinamento con la legge che tutela i minori dal *cyber*bullismo, e cioè la L. n. 71/2017, recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyber*bullismo".

[96] Ad esempio, fotografie e video artefatti con fotomontaggi imbarazzanti inviati a tutti i contatti dell'utente titolare dell'identità violata. Prima di esercitare tale rimedio, però, essi possono fare una segnalazione al *social network* tramite il previsto servizio *on line*, per chiedere la rimozione di ogni contenuto diffamatorio a loro carico. Rispetto, ad esempio, al *social network* Facebook, nel caso in cui tale segnalazione non dovesse sortire l'effetto sperato, l'utente può inviare ad esso una lettera raccomandata contenente una richiesta di accesso a tutti i dati che lo riguardano detenuti in relazione ai profili aperti a suo nome. Inoltre, se l'utente appartiene all'Unione Europea, può trasmettere un'istanza, ai sensi dell'art. 7 GDPR, per chiedere la conferma dell'esistenza e la comunicazione in forma intelligibile di tutti i dati che lo riguardano; ma anche per conoscere l'origine dei dati, le finalità, le modalità e la logica del trattamento, gli estremi identificativi del titolare e del responsabile, nonché i soggetti o le categorie di soggetti cui i dati sono stati comunicati o che possono venirne a conoscenza. Ancora, può pretendere la cancellazione e il blocco del falso *account* e dei dati illecitamente inseriti dallo stesso falso *account* e condivisi nel *social network*, chiedendo l'attestazione che tale operazione sia stata portata a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi. Infine, può presentare opposizione formale al trattamento dei dati in questione.

[97] Pertanto, al fine di consentire l'accertamento dei reati commessi e di bloccare la prosecuzione dell'attività criminosa (oltre che i contatti con altri utenti), il Garante per la protezione dei dati personali, in attesa di riuscire a

ISSN 2036-7821

La tutela dell'identità digitale da parte dell'ordinamento avviene, dunque, attraverso tecniche diverse e principalmente sotto due profili differenti: da un lato, attraverso l'impiego di sistemi di sicurezza informatica che impediscano l'accesso ad informazioni riservate; dall'altro, sotto il profilo dell'identità personale dell'utente, tramite la previsione normativa di principi e regole per gli operatori grazie ai quali garantire la liceità del trattamento dei dati. Ad ogni buon conto resta ferma la necessità che ciascun utente controlli i propri dati personali sul *web*, nella consapevolezza che è preferibile evitare i rischi *ab origine* piuttosto che dovervi, invece, porre rimedio dopo che si siano verificati.

8. L'attività della Pubblica Amministrazione e le conseguenze degli attacchi informatici tra difficoltà di prevenzione e di gestione.

La Pubblica Amministrazione ha il dovere di svolgere la sua attività perseguendo il principio della "buona amministrazione", che costituisce un diritto fondamentale della persona, riconosciuto come tale dall'art. 41 della Carta dei Diritti Fondamentali dell'Unione Europea[98].

Quello alla "buona amministrazione" rappresenta «*un principio guida dell'azione amministrativa, la cui nozione giuridica coincide con quell'idea filosofica secondo cui una buona Amministrazione Pubblica è un'amministrazione che adempie alle funzioni che le sono proprie nel contesto di una democrazia, ed è un'amministrazione che è al servizio dei cittadini e che svolge il proprio lavoro in maniera imparziale e razionale, giustificando le proprie azioni ed orientandosi continuamente all'interesse generale*»[99]. La digitalizzazione e l'utilizzo delle sempre più moderne tecnologie nel nostro Paese devono consentire, dunque, il miglioramento e la semplificazione dei procedimenti all'interno dei quali l'Amministrazione deve trattare e gestire le questioni che ineriscono al rapporto con i cittadini in modo equo, imparziale e trasparente. Del resto, anche la nostra

identificare il responsabile di essa, ordina al social di non effettuare un ulteriore trattamento e di conservare i dati finora trattati, senza provvedere lui stesso, autonomamente, alla loro cancellazione.

[98] Tale articolo prevede che ogni persona ha diritto a che «*le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione*», specificando che esso si sostanzi, ad esempio, nel diritto ad essere ascoltati prima che venga adottato un provvedimento individuale eventualmente pregiudizievole; o in quello di accedere al fascicolo nel rispetto dei legittimi interessi della riservatezza e del segreto professionale e commerciale.

[99] D. U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione. Il procedimento amministrativo, fra diritto UE e tecnologie ICT,* in (a cura di) R. CAVALLO PERIN e D. U. GALETTA, *Il diritto dell'amministrazione pubblica digitale,* Giappichelli, 2020, pp. 85-86. Per un approfondimento sul tema si vedano anche D. U. GALETTA, *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE),* in *Rivista italiana di diritto pubblico comunitario,* 2019, 2, p. 165 ss. F. TRIMARCHI BANFI, *Il diritto ad una buona amministrazione,* in M. P. CHITI, G GRECO (a cura di), *Trattato di diritto amministrativo europeo,* Giuffrè, Milano, 2007, pp. 63 ss.; A. ZITO, *Il «diritto ad una buona amministrazione» nella Carta dei diritti fondamentali dell'Unione europea e nell'ordinamento interno,* in *Rivista italiana di diritto pubblico comunitario*, 2002, pp. 427 ss. F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione,* in A. ROMANO (a cura di), *L'azione amministrativa. Saggi sul procedimento amministrativo,* Giappichelli, Torino, 2016.

Costituzione, all'art. 97, richiede che siano assicurati il buon andamento e l'imparzialità dell'azione amministrativa, e tali risultati sono conseguibili solo da parte di un'amministrazione efficiente, che, cioè, assume le proprie decisioni entro un tempo ragionevole e nel rispetto, nella tutela e nella garanzia degli interessi dei cittadini, singolarmente quanto collettivamente considerati.
Tra tali interessi deve esserci, ovviamente, anche quello a che quegli stessi strumenti che semplificano l'attività amministrativa e che il percorso di digitalizzazione ha reso possibile implementare nel nostro ordinamento non siano cd. "lame a doppio taglio" trasformandosi in strumenti che, invece, espongano a rischi gli interessi stessi mettendoli in pericolo.
Si è già detto che la Pubblica Amministrazione può diventare facilmente un "amo" attraverso cui fare abboccare vittime inconsapevoli che, ingannate da *e-mail* fraudolente - contraddistinte da loghi ad essa appartenenti ma che, in realtà, sono contraffatti, e partono da indirizzi di posta elettronica falsi - possono essere indotte ad immettere i dati richiesti e che saranno poi utilizzati per scopi non leciti.
In tali situazioni la Pubblica Amministrazione, anche se in maniera indiretta, è vittima delle frodi tanto quanto i destinatari delle *mail* stesse in quanto viene "strumentalizzata" dai criminali informatici che si avvalgono dello schermo dei suoi loghi per raggiungere il proprio obiettivo con maggiore possibilità di riuscita.
Il problema diventa più grave quando, invece, le condotte criminose sono specificamente indirizzate ad essa, in quanto, data la sua ontologica natura di "raccoglitore" di dati personali e sensibili dei cittadini, l'attacco informatico avrà inevitabili ripercussioni sulla collettività, i cui interessi saranno direttamente lesi. Infatti, se, come detto, ciascun individuo è personalmente responsabile della gestione della propria identità digitale e deve utilizzarla e tutelarla allo stesso modo di quella personale, parallelamente alla sua responsabilità di sarà, tanto più, quella della Pubblica Amministrazione, in quanto ad essa fa capo una molteplicità di interessi che appartengono ad un numero indefinito di individui, singolarmente o collettivamente considerati, della cui tutela e della cui protezione deve necessariamente farsi carico. Essa agisce per conto dei cittadini, ed il rapporto con questi è stato oggetto di importanti e determinanti disposizioni normative finalizzate a perfezionarlo e a semplificarlo, a cominciare già da quelle contenute nella legge sul procedimento amministrativo[100] che, gradualmente, è stato trasformato nel "luogo" della informatizzazione dei documenti amministrativi[101] al fine di rendere sempre più trasparente il rapporto tra la Pubblica Amministrazione ed i cittadini stessi[102].

[100] L. n. 241 del 1990.

[101] La disciplina relativa alla informatizzazione della Pubblica Amministrazione è stata introdotta nell'impianto della L. 241/90 grazie alla legge n. 15 del 2005, la quale vi ha inserito l'art. 3 *bis*, rubricato "Uso della telematica", da attuarsi all'interno della Pubblica Amministrazione, sia nei rapporti con altre P.A., che nei rapporti con i privati. Dello stesso anno, come già detto, è anche il Codice dell'Amministrazione digitale, introdotto, invece,

Nonostante il panorama normativo in tema di digitalizzazione sia, allo stato, ampio e sufficientemente implementato, l'emergenza sanitaria dell'ultimo anno ha, però, colto quasi impreparato il nostro Paese sotto questo aspetto, a causa, evidentemente, dell'assenza di un piano strutturato tramite il quale consentire a tutti i cittadini un equo accesso ai servizi digitali, non solo dal punto di vista materiale, ma anche da quello dell'istruzione all'utilizzo di essi. Una preparazione più adeguata avrebbe consentito, senza dubbio, una maggiore capacità di individuazione dei reali o potenziali attacchi ai sistemi informatici che ancora più frequentemente si sono verificati, ed avrebbe potuto anche tradursi nella possibilità di creare un rapporto di collaborazione tra cittadini e Pubblica Amministrazione, quasi in una sorta di reciproca difesa dalle problematiche in questione.
Oltre all'impreparazione generalizzata - conseguenza del già evidenziato "dilagante" analfabetismo digitale che deve, evidentemente, essere colmato e superato - però, la crisi pandemica ha evidenziato anche che non sussistono ancora, in capo all'Amministrazione, strumenti adeguati tramite cui gestire ed avvantaggiarsi della digitalizzazione, e dunque tali da consentirle di prevenire ed evitare che essa stessa sia esposta agli attacchi ai sistemi informatici.
L'Agid (Agenzia per l'Italia digitale)[103], infatti, ha reso noto che la maggior parte dei siti della Pubblica Amministrazione è seriamente esposta a rischi perché non è "sufficientemente sicura" (addirittura lo sarebbe solo il nove per cento di essi), e dunque i dati dei cittadini sono particolarmente vulnerabili[104]. L'Agenzia ha precisato che la causa di tale vulnerabilità vada ricercata negli stessi *software*, i quali, spesso, non sono aggiornati e sono mal configurati per cui, oltre a determinare disservizi e

tramite il D. Lgs. n. 80 del 14 maggio 2005, emanato a seguito della delega al Governo contenuta all'articolo 10 della legge 29 luglio 2003, n. 229, ed entrato in vigore nell'ordinamento italiano il 1° gennaio 2006. A proposito della digitalizzazione del procedimento amministrativo si vedano, *ex multis,* A. MASUCCI, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo ad istanza di parte,* Giappichelli, Torino, 2011; R. CAVALLO PERIN e I. ALBERTI, *Atti e procedimenti amministrativi digitali,* in (a cura di) R. CAVALLO PERIN e D. U. GALETTA, *Il diritto dell'amministrazione pubblica digitale,* Giappichelli, 2020, pp. 119-158; J. B. AUBY, *Il diritto amministrativo di fronte alle sfide digitali,* in *Istituzioni del Federalismo,* 2019, 3, pp. 619-641; C. NOTARMUZI, *Il procedimento amministrativo informatico,* in www.astrid-online.it, 2006.

[102] Interessante è, al riguardo, S. ROSSA, *Trasparenza e accesso all'epoca dell'amministrazione digitale,* in (a cura di) R. CAVALLO PERIN e D. U. GALETTA, *Il diritto dell'amministrazione pubblica digitale,* Giappichelli, 2020, pp. 247-275; ma si vedano anche B. PONTI (a cura di) *Nuova trasparenza amministrativa e libertà di accesso alle informazioni,* Rimini, 2016; M. A. SANDULLI, *Codice dell'azione amministrativa,* Milano, 2017.

[103] L'Agenzia per l'Italia digitale è stata istituita - tramite il D. L. 22 giugno 2012 n. 83 (cosiddetto "Decreto sviluppo") convertito in legge 7 agosto 2012 n. 134 - al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della Pubblica Amministrazione. In pratica, essa ha il compito di accreditare o autorizzare i soggetti (pubblici o privati) che svolgono attività in ambito digitale, quali, ad esempio, la conservazione sostitutiva, i certificati digitali, le marche temporali, le PEC, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

[104] Dati quali le credenziali di pagamento, i dati sanitari e qualsiasi altra informazione riservata.

discontinuità, sono anche facilmente attaccabili[105] tramite l'intrusione in essi, finalizzata non solo all'esfiltrazione di dati sensibili degli utenti del portale, ma anche all'infiltrazione di *malware* che possono addirittura portare ad un "sabotaggio" dell'intero sistema.

Il settore della Pubblica Amministrazione, in pratica, sembra essere quello maggiormente colpito ed aggredibile, ed i Comuni sono tra gli obiettivi più vulnerabili: rispetto ad essi il blocco di un qualsiasi servizio influisce direttamente sul benessere dei cittadini e si traduce non solo in perdite finanziarie, ma anche in altre conseguenze socialmente impattanti. Nel periodo di emergenza sanitaria, infatti, sono stati particolarmente frequenti attacchi realizzati attraverso strumenti informatici tecnologici che permettono di intercettare tutto ciò che viene digitato sulla tastiera di un *computer* anche se si trova in remoto (*keylogger*)[106]; attacchi in grado di rubare credenziali di accesso e dati sensibili, di spiare le vittime e di infettare i sistemi con una notevole velocità e varietà di *routine*[107]. Il vettore di diffusione "predefinito", anche in questo caso, è stato rappresentato dalle *e-mail* di *phishing*, ma anche via USB, dunque tramite le periferiche esterne di archiviazione.

I destinatari pubblici di queste condotte fraudolente sono stati vari, primo fra tutti l'INPS, oggetto di un serio e pericoloso attacco di *phishing* proprio nel pieno della crisi pandemica, quando cominciarono ad essere erogati da parte dell'Istituto i contributi economici necessari a "tamponare" le conseguenze delle interruzioni delle attività lavorative dovute al *lockdown*: attraverso tale attacco sono stati veicolati *malware* che hanno causato una serie di danni notevoli, tra cui la capacità di intercettare traffico di rete, di sottrarre credenziali ed anche di installare aggiuntivi codici malevoli.

Gli attacchi rivolti ad una Pubblica Amministrazione, allo stesso modo di quanto può accadere con una società, un'azienda o un privato cittadino, provocano certamente rilevanti danni economici e di violazione della *privacy*; ma quando l'Amministrazione attaccata è un ospedale, le conseguenze possono essere molto più gravi, perché ad essere coinvolta è la salute degli individui, diritto ed interesse fondamentale ed inviolabile, al quale sono legate informazioni confidenziali e sensibili, aventi, purtroppo, un alto valore remunerativo nel *Dark Web*. Le strutture

[105] I dati evidenziati dall'Agid sono il frutto degli studi richiesti dal Piano triennale per l'informatica 2020-2022, dai quali è emerso che, a fronte della esigua percentuale del 9% di siti sicuri, addirittura il 67% dei domini pubblici presenta "gravi problemi" ed il 22% è "mal configurato".

[106] Secondo i dati contenuti nel *Threat Intelligence Report* 3Q2020, elaborato dall'Osservatorio *CyberSecurity* di *Exprivia*, infatti, nel periodo luglio-settembre del 2020 sono stati registrati 148 attacchi, incidenti e violazioni della *privacy*, rispetto ai 171 eventi del periodo aprile-giugno e ai 49 tra gennaio e marzo dello stesso anno. Così come ce ne sono stati molti anche nel primo semestre del 2021: si ricorda, tra quelli più gravi, l'attacco *ransomware* ai sistemi informativi della Regione Lazio - infrastruttura critica che rientra nel perimetro della Direttiva NIS del 2016.

[107] Specificamente si fa riferimento a *MassLogger*, il *keylogger* che ruba credenziali di accesso e dati sensibili sia ad utenti privati che ad utenze della Pubblica Amministrazione.

ISSN 2036-7821

sanitarie, inoltre, oltre ad essere tra le più attrattive per il *cyber crime* proprio per questo motivo, rappresentano anche un bersaglio ancora più facile da cogliere rispetto alle altre amministrazioni, perché i sistemi informativi sanitari, nel mentre sono generalmente attenti a rispettare le normative sulla *privacy*, non sono, invece, progettati e gestiti in modo da resistere ad attacchi informatici mirati, rendendo la sanità poco protetta e, dunque, vittima perfetta per i *cyber*criminali[108]. Pertanto, il blocco dei sistemi informativi ospedalieri che consegue ad un attacco di *ransomware* riesce concretamente a minare la capacità operativa della struttura che ne è vittima, mettendo, ovviamente, a rischio la salute dei pazienti, perché il *ransomware*, una volta infiltratosi in una rete, provvede a cifrare tutti i dati che riesce a trovare sui sistemi raggiungibili da quella stessa rete, provocandone il blocco totale almeno fino a quando non sarà stato pagato, all'organizzazione criminale che ha condotto l'attacco, il riscatto che consentirà di ottenere, in cambio, la specifica chiave in grado di decifrare i dati virtualmente "sequestrati"[109].

Se da un attacco *ransomware* ad una struttura ospedaliera deriva la morte di un paziente, esiste una norma che punisce tale condotta, e cioè quella di omicidio contenuta nel codice penale; ma è altrettanto necessario che sussistano strumenti e misure di natura preventiva ed obbligatoria grazie ai quali evitare in radice che si verifichino episodi gravi di tal genere; e, dunque, se, effettivamente, la causa principale di essi è da ascriversi a sistemi *software* poco robusti ed aggiornati, una prima soluzione dovrebbe, evidentemente, essere quella di investimenti maggiori e più costanti nel tempo, sia di natura economica che sotto forma di risorse umane, e che, specie nella *cybersecurity*, finora non sono ancora stati così rilevanti.

L'emergenza Covid-19 si è rivelata un'occasione propizia all'aumento degli attacchi informatici, che avrebbero, invece, potuto essere contrastati con maggiore decisione se ci fosse stato un più elevato livello di conoscenza e di formazione sulla sicurezza. Tale imprevisto ed imprevedibile accadimento, paradossalmente, tra le gravi conseguenze che ha determinato, ha anche evidenziato che è necessario investire a tutti i livelli in cultura digitale, in misure proattive che accrescano la consapevolezza e le competenze per riconoscere un crimine e, soprattutto, per fare in modo che esso non si verifichi.

La digitalizzazione di un Paese non può limitarsi solo a predisporre le norme giuridiche che la prevedono. Essa dipende da numerosi fattori: da quelli infrastrutturali, legati alla disponibilità sul territorio di una rete in banda ultra larga sicura, efficiente ed accessibile a cittadini e imprese; a quelli culturali, relativi alla

[108] Tanto è vero che si è registrato che gli attacchi ad essa sono aumentati talmente tanto da arrivare alla percentuale del 38% nel terzo trimestre del 2020.

[109] Purtroppo, anche in Italia sono stati registrati attacchi *ransomware* diretti ad ospedali; specificamente, allo Spallanzani di Roma - episodio che si è verificato nelle prime fasi dell'esplosione della pandemia, e cioè a marzo 2020 -, ed al Fatebenefratelli di Erba, nel dicembre 2019.

ISSN 2036-7821

diffusione delle competenze digitali e al radicamento di una mentalità "digitale" nel contesto economico e sociale; a quelli, infine, di sistema, legati alla presenza di normative capaci di governare il cambiamento nell'ottica di stimolare l'innovazione a tutti i livelli. Rispetto a tali fattori, la Pubblica Amministrazione ha, senza dubbio, cambiato il proprio approccio che, infatti, denota una maggiore consapevolezza circa la necessità di creare un modello organico, nel quale confluiscano indirizzi e piani nazionali che comprendano tutti i fattori chiave e che la pongano al centro del cambiamento. Ma, evidentemente, il percorso da compiere è ancora lungo. L'obiettivo a cui si deve tendere, infatti, è quello di allinearla alle stesse logiche aziendali in materia di sicurezza informatica: in pratica, bisognerebbe integrare il *cyber risk* all'interno dell'*enterprise risk management framework* aziendale (ERM)[110], partendo dalla definizione di una strategia precisa e con un processo gestionale rigoroso, grazie al quale riuscire a comprendere che il *cyber risk* non è un rischio residuale, ma è uno dei più critici, relativamente al quale non sono più tollerabili né la scarsa consapevolezza del reale valore delle informazioni trattate, né la non adeguatezza a sostenere una corretta strategia di mitigazione del rischio degli investimenti tecnologici, né, infine, la scarsa preparazione del personale su questi temi.
È necessario un approccio basato su una maggiore *governance* e gestione del rischio: in pratica, è necessario che le amministrazioni comprendano che ad un progetto di sviluppo digitale si debba affiancare sempre una corretta strategia di *security;* e che l'*Information security* debba divenire parte del processo organico di sviluppo digitale di qualsiasi Pubblica Amministrazione.

9. *Le prospettive di riforma della* cyber*sicurezza contenute nel PNRR.*
La situazione attuale in materia di sicurezza informatica non consente di ravvisare ancora una perfetta corrispondenza tra ciò che dovrebbe essere in teoria e quello che, invece, è nella realtà; e la ragione è che non sembra essere ancora del tutto chiaro che è l'intera organizzazione amministrativa a dovere essere radicalmente modificata, attraverso un forte coinvolgimento innanzitutto dei *manager* pubblici che, concretamente, possono e devono provvedere all'analisi quantitativa del rischio sì da renderne reale il valore economico e, valutandolo in rapporto ai benefici, da potere intraprendere le azioni più opportune e fare gli investimenti più adeguati.
Solo grazie a questa evoluzione la Pubblica Amministrazione potrà svolgere il ruolo fondamentale e centrale che ci si attende da essa nella ripresa del Paese dalle conseguenze della pandemia grazie ai fondi europei e che è contenuto nel Piano Nazionale di Ripresa e Resilienza (PNRR) - elaborato dal Governo italiano e

[110] L'ERM è una disciplina di gestione del rischio aziendale che mantiene allineata l'organizzazione alle strategie per il perseguimento degli obiettivi e, proprio per questa sua natura, rappresenta uno strumento di *governance* aziendale.

ISSN 2036-7821

sottoposto alle istituzioni europee alla fine del mese di aprile 2021, per accedere ai fondi di Next Generation EU (NGEU)[111].

Esso contempla, tra le sue Missioni, proprio quella di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese[112], ed a tale fine prevede un intervento profondo, che agisca innanzitutto sulla connettività per cittadini, imprese e pubbliche amministrazioni, ma anche sulla modernizzazione della Pubblica Amministrazione nell'ambito del sistema produttivo.

In particolare, la Missione 1 - indirizzata specificamente alla "Digitalizzazione, innovazione, competitività e cultura"[113] - nella prima delle tre componenti di cui è costituito ha, infatti, come obiettivo la digitalizzazione e la modernizzazione della P.A. attraverso lo sviluppo di un *cloud* nazionale e la effettiva interoperabilità delle banche dati di queste in parallelo e in sinergia con il progetto Europeo GAIA-X, all'interno del quale l'Italia intende avere un ruolo di primo piano.

Tale progetto introduce il nuovo *cloud* d'Europa[114]: in pratica, esso vuole realizzare un'infrastruttura, a livello europeo, il cui fine è quello di raggiungere la sovranità digitale europea nel campo del *cloud*, fornendo a tutti i Paesi *partner* uno standard unico e che sarà da questi condiviso per garantire la sicurezza dei dati dei Paesi UE, collegando tra di loro i diversi servizi in *cloud* e dando luogo ad una Federazione efficiente e competitiva di infrastrutture di dati e fornitori di servizi in ambito UE.

L'obiettivo, dunque, è quello di raggiungere un elevato livello di digitalizzazione per completare il percorso delle riforme della Pubblica Amministrazione[115] e realizzare un vero e proprio cambiamento strutturale, organico e integrato, ai diversi livelli di governo, che la trasformi in amministrazione competente, semplice, *smart* e soprattutto capace di offrire servizi di qualità ai cittadini e alle imprese.

Ma perché questo obiettivo si realizzi non è necessario solo agire sugli aspetti di "infrastruttura digitale", spingendo la migrazione al *cloud*[116] delle amministrazioni,

[111] I fondi di Next Generation EU (NGEU) rappresentano il nuovo strumento dell'Unione europea per la ripresa che integra il Quadro finanziario pluriennale per il periodo 2021-2027.

[112] Tale è il contenuto della Missione 1.

[113] Tale missione – che si struttura in 3 componenti - si pone come obiettivo la modernizzazione del Paese, abbracciando la rivoluzione digitale, sia nella Pubblica Amministrazione sia nel suo sistema produttivo, le necessarie riforme "di sistema", quella della Giustizia e la piena realizzazione di quella della P.A., e – infine – investendo nei settori che più caratterizzano l'Italia e ne definiscono l'immagine nel mondo: il turismo e la cultura.

[114] Esso è stato presentato per la prima volta al Digital Summit 2019 a Dortmund, in Germania.

[115] Per la realizzazione di tali riforme andrà sviluppato un "Programma di innovazione strategica della P.A.", secondo le previsioni del PNRR.

[116] Il *cloud* rappresenta il *server* grazie al quale, accedendovi tramite *Internet*, gli utenti e le imprese hanno la possibilità di gestire il *software* e i *database* che si trovano su di esso e dunque di accedere agli stessi file e alle stesse applicazioni da ogni dispositivo e da dovunque si trovino, perché l'elaborazione e l'archiviazione dei dati hanno luogo in *server* che si trovano in *datacenter* nel dispositivo dell'utente.

ISSN 2036-7821

accelerando l'interoperabilità tra gli enti pubblici e snellendo le procedure[117]; è, altresì, necessario anche rafforzare le difese di *cybersecurity*.

La promozione dell'innovazione e della digitalizzazione del sistema produttivo attraverso incentivi agli investimenti in tecnologia, ricerca e sviluppo rappresenta, dunque, un passaggio strumentale alla realizzazione di un modello di Amministrazione più efficiente, e siccome, come detto, dalla digitalizzazione deriva, purtroppo, anche l'aumento del livello di vulnerabilità della società rispetto a minacce *cyber*, (sotto forma di frodi, ricatti informatici, attacchi terroristici ed altro), il PNRR prevede non solo un Investimento[118] destinato proprio alla *cybersecurity*, attraverso il quale introdurre importanti misure di rafforzamento delle difese *cyber* del Paese, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica[119]"; ma anche un Investimento relativo alle

[117] Ad esempio evitando di chiedere a cittadini ed imprese informazioni già fornite in precedenza, in base al principio del "*once only*."

[118] L'Investimento in questione è l'1.5. Segnatamente, gli investimenti sono organizzati su quattro aree di intervento principali: innanzitutto il rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la Pubblica Amministrazione e le imprese di interesse nazionale. In secondo luogo, si vuole costruire o rendere più solide le capacità tecniche di valutazione e *audit* continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale. Inoltre, si vuole investire nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il Paese da minacce cibernetiche. Infine, si prevede di irrobustire gli *asset* e le unità *cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

[119] Il perimetro di sicurezza nazionale cibernetica è stato istituito attraverso il D.L. n. 105 del 2019 - convertito nella legge n. 133 del 2019 - successivamente emendato con il cd. decreto "milleproroghe" 2020, ovvero il D.L. 30 dicembre 2019, n. 162 (convertito, con modificazioni, dalla L. 28 febbraio 2020, n. 8). In realtà, la definizione di esso è stata rinviata ad un d.p.c.m. da adottare su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), entro la "cornice" indicata dal decreto legge. In ogni caso, la *ratio* sottesa alla sua istituzione è quella di 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, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale*», nonché a criteri che dovranno essere rispettati nella definizione. Tali criteri sono: l'individuazione di soggetti che esercitano una funzione essenziale dello Stato, ovvero assicurano un servizio essenziale per il mantenimento delle attività civili, sociali o economiche fondamentali per gli interessi dello Stato; la dipendenza dell'esercizio di tale funzione o della prestazione del servizio da reti, sistemi informativi e servizi informatici; la gradualità in rapporto all'entità del pregiudizio per la sicurezza nazionale ed in relazione alle specificità dei diversi settori. L'atto amministrativo con il quale vengono indicati tali criteri è sottratto all'accesso e non è soggetto a pubblicazione, ferma la separata comunicazione data a ciascun soggetto inserito nel perimetro, senza ritardo, dell'avvenuta iscrizione nell'elenco. Come evidenziato in dottrina, tale sottrazione ha, evidentemente, lo scopo di garantire e tutelare la sicurezza nazionale, in linea con la previsione dell'art. 24 della l. n. 241 del 1990. Cfr. B. BRUNO, Cybersecurity *tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, su www.federalismi.it, n. 14/2020, 26 ss.

Competenze digitali di base[120] che avrà, invece, lo scopo di migliorare il livello di alfabetizzazione digitale in maniera generalizzata.
Insomma, la Pubblica Amministrazione ha l'obbligo di "migliorare" per stare al passo con la nuova realtà e di conoscere e predisporre strumenti di difesa e di contrasto delle minacce diversi da quelli che sono stati utilizzati fino ad ora - come, ad esempio, gli *antimalware*, o il controllo del traffico e della posta elettronica – e che sono stati dei "rimedi" adottati successivamente al verificarsi delle minacce stesse, piuttosto che degli strumenti di prevenzione.
Nell'implementazione di sempre più evoluti processi di digitalizzazione, la Pubblica Amministrazione deve garantire il costante aggiornamento dei sistemi e deve predisporre adeguate misure di sicurezza, educando e sensibilizzando i dipendenti alle tematiche della *cybersecurity* - e cioè alle minacce informatiche e alle modalità di contrastarle - affinché i loro errori e la loro impreparazione non siano la causa del mancato miglioramento dei processi.
In un'ottica di "*cyber*-resilienza", in pratica, la Pubblica Amministrazione deve, da un lato, assicurare la protezione dell'interesse pubblico per i dati personali e sensibili degli interessati-cittadini, attraverso la protezione dei sistemi; e, dall'altro, deve garantire l'esistenza di un sistema di recupero celere grazie al quale ripristinare lo *status quo ante* nel caso in cui essa resti vittima di un attacco che determini la perdita di disponibilità o dell'integrità o della riservatezza delle informazioni e che possa avere come conseguenza la compromissione del naturale e costante prosieguo dell'attività pubblica, ostacolando, di fatto, l'attuazione del diritto alla "buona amministrazione" richiesto per la migliore soddisfazione degli interessi pubblici.

10. I recentissimi interventi normativi in materia di sicurezza informatica a livello europeo e nazionale.
Gli evidenziati obiettivi che il PNRR si propone di realizzare per raggiungere un modello di Amministrazione più efficiente possono essere conseguiti solo attraverso una consapevole azione congiunta da parte di tutti gli Stati membri dell'Unione europea ed una adeguata individuazione delle specifiche competenze all'interno di ciascuno di essi.
Tali auspicabili risultati sono gli obiettivi di due recentissimi atti normativi, uno di livello europeo ed uno di livello nazionale, e cioè il Regolamento (UE) 2021/887, che istituisce il Centro Europeo di competenza per la *cyber*sicurezza, e la Legge 109/2021 che istituisce l'Agenzia per la *cyber*sicurezza nazionale.
a) *Il Regolamento (UE) 2021/887 istitutivo del Centro Europeo di competenza per la* cyber*sicurezza*

[120] Investimento 1.7.

ISSN 2036-7821

L'Unione Europea, il 20 maggio 2021, ha emanato un atto di fondamentale importanza e che rappresenterà un imprescindibile punto di riferimento per tutti i Paesi dell'Unione; si tratta del Regolamento (UE) 2021/887 del Parlamento Europeo e del Consiglio, che istituisce il "Centro europeo di competenza per la *cyber*sicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento", ovvero un atto normativo emanato su un presupposto indefettibile, e cioè la consapevolezza che «*la maggior parte della popolazione dell'Unione è collegata a Internet*» e che «*la vita quotidiana delle persone e le economie dipendono sempre di più dalle tecnologie digitali*» con la conseguenza che non solo i cittadini ma anche le imprese sono sempre più esposti a gravi incidenti di *cyber*sicurezza[121].

Partendo da questa premessa, l'Unione Europea fornisce gli Stati membri dello strumento che possa loro consentire di potenziare le «*capacità tecnologiche e* industriali» ricorrendo a «*standard elevati e soluzioni olistiche in materia di cybersicurezza che coinvolgano le persone, i prodotti, i processi e le tecnologie dell'Unione*», ma anche di «*una leadership dell'Unione negli ambiti della cybersicurezza e dell'autonomia digitale*». In pratica, grazie al Centro di competenza che istituisce con tale Regolamento, l'Unione si prefigge l'obiettivo di coinvolgere tutti gli Stati nell'adozione di azioni congiunte in materia di sicurezza informatica, sensibilizzandoli circa le minacce rivolte alla sicurezza ed all'autonomia digitale e stimolandoli allo sviluppo di competenze, capacità e abilità, «*tenendo pienamente conto delle implicazioni e preoccupazioni sociali ed etiche*».

Come è noto, gli interventi normativi a livello europeo, che pure hanno svolto un indubbio ruolo nell'identificazione dei profili nevralgici e nella promozione di un approccio unitario in materia di sicurezza informatica, hanno, però, affrontato il tema con prudenza ed anche un po' di lentezza.

Infatti, prima di istituire l'Agenzia europea per la sicurezza delle reti e dell'informazione grazie al Reg. CE n. 460/2004 - ENISA - si sono registrati solo normative o prescrizioni non vincolanti per gli Stati membri. Tale Agenzia è stata inizialmente configurata quale organo tecnico di assistenza alla Commissione europea ed agli Stati membri; successivamente, con il reg. CE n. 526/2013[122] il suo ruolo è stato rilanciato fino al giugno del 2020, pur lasciando ampio spazio di manovra agli Stati membri[123], ma è solo con il Regolamento (UE) 2019/881 (c.d. *Cybersecurity act*), che essa ha finalmente assunto confini operativi più definiti.

---

[121] Considerando 1.

[122] Reg. (CE) 21-5-2013 n. 526/2013, Regolamento del Parlamento e del Consiglio relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

[123] B. BRUNO, Cybersecurity *tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, cit. che evidenzia che non sono stati molti gli atti rilevanti dell'ENISA e che tra questi va menzionato quello del dicembre del 2012, il report "*National Cyber Security Strategies. Practical Guide on Development and Execution*", perché è quello che ha poi fornito il quadro di riferimento per I documenti programmatici italiani in materia di *cybersecurity*.

ISSN 2036-7821

Va, però, evidenziato che è del 2013 anche la «Strategia dell'Unione europea per la *cyber*sicurezza: un *cyber*spazio aperto e sicuro» («Strategia per la *cyber*sicurezza del 2013») - intesa a promuovere un ecosistema cibernetico affidabile, sicuro e aperto – mentre sono del 2016 le prime misure nel settore attraverso la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio sulla sicurezza delle reti e dei sistemi informativi[124], che ha previsto i primi meccanismi di cooperazione strategica e operativa tra gli Stati membri, oltre che alcuni obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti nei principali settori strategici a livello economico e sociale. L'Italia l'ha recepita con il D. Lgs. n. 65 del 2018, che, però, poco ha inciso sulle dinamiche del mercato e dei *market players* digitali.

Nel 2017, l'Unione Europea è stata invitata a diventare un *leader* mondiale in materia di sicurezza informatica entro il 2025, al fine di garantire la fiducia, la sicurezza e la tutela dei cittadini, dei consumatori e delle imprese *online* e «*di fare sì che Internet sia libero, più sicuro e regolamentato*», ma tale obiettivo, come si evidenzia nello stesso Regolamento (UE) 2021/887, purtroppo, allo stato, non è ancora raggiungibile, in quanto mancano capacità e mezzi tecnologici sufficienti grazie ai quali raggiungerlo, e tale insufficienza è, a sua volta, causata da investimenti frammentari e da un accesso assai limitato alle conoscenze, alle competenze ed alle strutture in materia che determinano scarsi risultati sulla ricerca e sull'innovazione che possano tradursi in soluzioni commercializzabili o di ampia diffusione in tutti i comparti economici.

La *ratio* sottesa all'istituzione del Centro di competenza[125] è, dunque, quella di concentrare gli investimenti nello sviluppo industriale, nella tecnologia e nella ricerca sulla *cyber*sicurezza, al fine di attuare progetti e iniziative pertinenti in collaborazione con la rete[126] e di fornire l'adeguato sostegno finanziario attraverso sinergie e coordinamenti che evitino inutili duplicazioni. Sarà, infatti, il Centro di competenza ad agevolare lo sviluppo di infrastrutture, pur non dovendo esso svolgere direttamente compiti operativi quali quelli connessi ai gruppi di intervento per la sicurezza informatica in caso di incidenti (CSIRT), compresi il monitoraggio e la gestione di questi.

In pratica, il Centro è un organismo dotato di personalità giuridica[127] - la cui durata sarà limitata al periodo compreso fra il 28 giugno 2021 e il 31 dicembre 2029 - il quale, insieme con la Rete e la Comunità, dovrebbe contribuire al progresso e alla diffusione dei prodotti, servizi e processi per la sicurezza informatica, promuovendo, al

[124] Nota come direttiva NIS "*network and information security*".

[125] Esso ha sede a Bucarest e, ai sensi dell'art. 11 del Regolamento, ne sono membri l'Unione, rappresentata dalla Commissione, e gli Stati membri; la sua struttura comprende un consiglio di direzione, un direttore esecutivo ed un gruppo consultivo strategico.

[126] Per "rete" si intende quella costituita dai vari centri nazionali di coordinamento che il Regolamento vuole che siano istituiti in ciascuno Stato membro al fine di coadiuvare il Centro di competenza.

[127] Ad esso si applica il regolamento delegato (UE) 2019/715 della Commissione.

ISSN 2036-7821

contempo, ove possibile, l'attuazione del quadro europeo di certificazione della *cyber*sicurezza istituito dal Regolamento (UE) 2019/881.

Gli Stati sono investiti della responsabilità di contribuire al finanziamento del Centro di competenza anche attraverso sovvenzioni concesse da uno Stato membro ad un beneficiario in tale Stato[128], sì da integrare il sostegno finanziario dell'Unione ad un progetto nell'ambito del programma di lavoro annuale; è previsto, altresì, che, qualora un ente di uno Stato membro sia esso stesso beneficiario di un sostegno finanziario dell'Unione, saranno possibili anche contributi in natura, vale a dire contributi che corrispondono alle «*spese ammissibili sostenute dai centri nazionali di coordinamento e da altri enti pubblici quando questi partecipano a progetti finanziati dal regolamento, laddove tali spese non sono finanziate mediante un contributo dell'Unione o un contributo finanziario degli Stati membri*»[129].

Il Regolamento, inoltre, si preoccupa di fornire tutte le definizioni necessarie ed essenziali al fine di comprendere in maniera adeguata le problematiche connesse al tema della sicurezza informatica, riprendendo, ad esempio, quella relativa a cosa sia una "minaccia informatica"[130] ma anche cosa si intenda per "azione congiunta"[131].

Le funzioni ed i compiti attribuiti al Centro di competenza saranno svolte congiuntamente con gli Stati membri: infatti, l'art. 6 prevede che, entro il 29 dicembre 2021, ciascuno di essi designi un centro nazionale di coordinamento, vale a dire un ente (che può essere anche già situato in tale Stato membro) che appartenga al settore pubblico o sia a partecipazione pubblica maggioritaria e che eserciti funzioni amministrative pubbliche ai sensi del diritto nazionale, anche per delega. Esso deve essere in grado di sostenere il Centro di competenza e la rete nell'assolvimento della loro missione, disponendo di competenze in materia di *cyber*sicurezza nell'ambito della ricerca e della tecnologia.

In pratica, i vari centri nazionali fungono da punti di contatto a livello nazionale per la comunità ed assistono il Centro di competenza nel conseguimento dei suoi obiettivi e dei suoi compiti strategici, tra i quali, ad esempio, quello di sviluppare e monitorare l'attuazione dell'"agenda"[132].

---

[128] Considerando 52.

[129] Art. 1.

[130] Già definita come «*qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone*» dall'art. 2, punto 8) del citato Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 19 aprile 2019 relativo all'ENISA, l'Agenzia europea per la *cyber*sicurezza.

[131] Si tratta di «*un'azione prevista nel programma di lavoro annuale che riceve un sostegno finanziario a titolo di Orizzonte Europa, del Programma Europa digitale o di altri programmi dell'Unione, nonché un sostegno finanziario o in natura da parte di uno o più Stati membri, ed è attuata mediante progetti che coinvolgono beneficiari stabiliti in tali negli Stati membri e che ricevono un sostegno finanziario o in natura ai beneficiari provenienti dai medesimi Stati membri*».

[132] L'agenda è definita, all'art. 1, come la strategia di cybersicurezza «in materia industriale, tecnologica e della ricerca globale e sostenibile, che formula raccomandazioni strategiche per lo sviluppo e la crescita del settore europeo della cybersicurezza nell'ambito industriale, tecnologico e della ricerca, e che contiene le priorità

ISSN 2036-7821

Oltre ai Centri nazionali, un ruolo importante è attribuito alla Comunità delle competenze in materia di *cyber*sicurezza; quest'ultima è costituita da organizzazioni industriali - comprese le PMI - accademiche e di ricerca, da altre associazioni pertinenti della società civile, ma anche da organizzazioni europee di normazione ed enti pubblici che si occupano di questioni operative e tecniche in materia di *cyber*sicurezza[133]. Anche la Comunità contribuisce alla missione del Centro di competenza e della Rete consolidando, condividendo e divulgando le competenze in materia di *cyber*sicurezza in tutta l'Unione.

Sia le azioni del Centro di competenza che quelle dei Centri nazionali e della Comunità devono essere improntate alla massima trasparenza, in quanto il pubblico e le parti interessate devono poter disporre tempestivamente di informazioni adeguate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del loro lavoro, potendo eventualmente anche presenziare in qualità di osservatori allo svolgimento di alcune attività.

Il Regolamento *de quo* segna, dunque, un passaggio importante in materia di sicurezza informatica, non solo perché istituisce un soggetto giuridico - il Centro di competenza, appunto - che deve svolgere la "missione" di coordinare le azioni di tutti gli Stati membri, ma anche perché, per la prima volta, evidenzia la necessità che esista una rete di soggetti, facenti capo ai singoli Stati stessi, che provveda a coordinare a livello nazionale le attività da implementare e che collabori con il Centro di competenza.

In pratica, attraverso tale atto normativo l'Unione europea ha investito ciascuno Stato della responsabilità di "fare gruppo" e di interagire su una tematica delicata, complessa ed ancora non adeguatamente studiata e compresa quale quella della *cybersecurity*, relativamente alla quale l'azione individuale non può essere efficace tanto quanto quella congiunta.

b) *La Legge 109/2021 istitutiva dell'Agenzia per la cybersicurezza nazionale*

L'atto normativo di livello nazionale cui si è fatto cenno, invece, è la Legge 4 agosto 2021, n. 109, che, in realtà, è la legge di conversione del D. L. 82/2021 che è, per l'appunto, intitolata "Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di *cyber*sicurezza, definizione dell'architettura nazionale di *cyber*sicurezza e istituzione dell'Agenzia per la *cyber*sicurezza nazionale"[134]; anche all'interno di tale disciplina, come nel Regolamento (UE) 2021/887, sono contenute le definizioni essenziali ai fini della comprensione del tema, prima fra tutte quella relativa proprio alla

strategiche per le attività del Centro di competenza e non è vincolante per quanto attiene alle decisioni da adottare riguardo ai programmi di lavoro annuali».

[133] Art. 8.

[134] L'istituzione di tale Agenzia era già stata prevista dalla Direttiva NIS e dal Reg. 881/2019, ma solo nel 2021 si è concretizzata.

"*cyber*sicurezza"[135], ma anche quella relativa alla "resilienza nazionale nello spazio cibernetico"[136].

Tale legge, per la prima volta, individua ed attribuisce specificamente le competenze in materia di sicurezza informatica nazionale, istituendo, altresì, *ex novo* un soggetto deputato alla tutela ed alla garanzia di questo rilevante settore, vale a dire l'Agenzia per la *cyber*sicurezza nazionale.

Segnatamente, infatti, viene investito del potere di alta direzione e di responsabilità generale delle politiche di *cyber*sicurezza il Presidente del Consiglio dei Ministri, al quale competono l'adozione della strategia nazionale in materia - sentito il Comitato interministeriale per la *cyber*sicurezza (CIC)[137] - e la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia, previa deliberazione del Consiglio dei ministri.

All'Agenzia, invece, competono i compiti di coordinamento tra i soggetti pubblici coinvolti in materia di *cyber*sicurezza a livello nazionale e di promozione della realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni.

Essa assume le funzioni di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e svolge attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi e della sicurezza delle reti di comunicazione elettronica.

Può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze armate, di quelle di Polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali[138].

Presso l'Agenzia è costituito, in via permanente, il "Nucleo per la *cyber*sicurezza", a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla

---

[135] Definita come l'insieme delle attività e degli obblighi derivanti da trattati internazionali, necessari per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

[136] Con la quale si intendono le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131.

[137] Tale Comitato è istituito ai sensi dell'art. 4 della legge in questione.

[138] L'Agenzia ha sede a Roma ed è dotata di personalità giuridica di diritto pubblico e di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. Il suo direttore generale – che deve essere in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione - dura in carica quattro anni, rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. Si evidenzia, inoltre, che l'Agenzia è posta sotto il diretto controllo del COPASIR (Comitato Parlamentare per la Sicurezza della repubblica); essa è istituita in capo alla Presidenza del Consiglio dei Ministri ed avrà personale *ad hoc* anche non proveniente dalla Pubblica Amministrazione: in particolare, il suo organico sarà composto inizialmente da 300 dipendenti.

prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Tale soggetto ha il compito di gestire in maniera unitaria le situazioni di crisi cibernetica (come quella che si è verificata durante la recente pandemia) e di assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto ad esse vengano espletate in maniera coordinata, mantenendo costantemente informato il Presidente del Consiglio dei ministri e raccogliendo ed elaborando rapporti e dati relativi alla crisi rispetto ai quali fornire informazioni. Il Nucleo deve, inoltre, provvedere a trasmettere tutti questi dati ai soggetti pubblici e privati interessati e deve partecipare ai meccanismi europei di gestione delle crisi cibernetiche, coordinandosi con gli omologhi organismi di altri Stati, della NATO, dell'Unione europea o di organizzazioni internazionali di cui l'Italia fa parte.

Va evidenziato, inoltre, che, in materia di trattamento dei dati personali, la legge *de qua* prevede espressamente che ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano le disposizioni del Codice della *Privacy*[139] concernenti i controlli relativi ai trattamenti di dati personali effettuati dal DIS, AISE e AISI[140] e di dati coperti da segreto di Stato. In base a tali disposizioni, il componente designato[141] per gli accertamenti dal Garante per la protezione dei dati personali deve prendere visione degli atti e dei documenti rilevanti e riferire oralmente nelle riunioni del Garante[142].

Al di là delle critiche che, inevitabilmente, sono state fatte a tale Legge circa la sua completezza, il suo pregio è avere dimostrato, per la prima volta, un interesse concreto da parte del Legislatore nazionale al tema della sicurezza informatica, pur nella consapevolezza che esso debba essere trattato ed abbia una dimensione extranazionale e globale, per cui i soggetti che si appropriano di siti altrui non sono quasi mai criminali di estrazione nazionale, ben radicati in una individuabile area geografica, ma sono criminali che abitano un luogo indefinito, per convenzione chiamato "*dark web*".

Precedentemente ad essa, oltre ai già citati D. Lgs. n. 65/2018 di recepimento della Direttiva (UE) 2016/1148 e D.L. n. 105 del 2019 in tema di *cyber*sicurezza, gli interventi normativi italiani sono stati forse ancora più prudenti di quelli europei e, soprattutto, sono stati prevalentemente orientati alla difesa della Pubblica

[139] E cioè il comma 1, dell'art. 58 del Codice della *Privacy*.

[140] E cioè, rispettivamente, il Dipartimento delle informazioni per la sicurezza, l' Agenzia informazioni e sicurezza esterna e l'Agenzia informazioni e sicurezza interna, tutti organismi previsti dalla legge 3 agosto 2007, n. 124.

[141] Designato tramite il richiamo all'art. 160, comma 4 del Codice *Privacy*.

[142] Art. 13: «*Il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione del presente decreto è effettuato ai sensi dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196*».

Amministrazione e della sicurezza nazionale, senza, però, fornire soluzioni operative in tema di sicurezza della libertà del singolo cittadino o di tutela dei diritti e modalità di esercizio degli stessi.

Si fa riferimento, in particolare, agli interventi del 2013, e cioè i primi indirizzi ufficiali del Governo in materia di *cybersecurity*[143], con i quali si è definita l'architettura istituzionale deputata alla tutela della sicurezza nazionale circa le infrastrutture critiche materiali e immateriali; ma anche al "Quadro strategico nazionale per la sicurezza dello spazio cibernetico"[144] - che individua profili e tendenze evolutive della *cybersecurity*, definendo ruoli e compiti affinché possa esserci compartecipazione tra i diversi soggetti pubblici e privati nel contrasto alle minacce informatiche - ed al "Piano nazionale per la protezione cibernetica e la sicurezza informatica" - che, invece, individua strumenti e procedure per potenziare le capacità cibernetiche dell'Italia, attraverso sei indirizzi strategici e undici indirizzi operativi.

Ma si fa riferimento anche alla Direttiva 1 agosto 2015 della Presidenza del Consiglio dei Ministri, tramite la quale è stato precisato il quadro d'insieme dell'attività di *cyber*sicurezza, fissando linee d'azione per i soggetti coinvolti e conferendo non solo maggiore attenzione alle azioni per il partenariato pubblico-privato - seppure sempre in termini molto generici - ma anche riconoscendo, per la prima volta, che il tema della *cybersecurity* è una questione di garanzia per i diritti fondamentali degli individui costituzionalmente protetti e non una mera questione di "difesa nazionale"[145].

Del 2017, invece, è il d.p.c.m. con il quale è stata ridefinita l'architettura nazionale della sicurezza cibernetica, con rafforzamento, tra l'altro, del ruolo del CISR (Comitato interministeriale per la sicurezza della Repubblica) e riconduzione del Nucleo Sicurezza Cibernetica (NSC) all'interno del Dipartimento delle informazioni per la sicurezza (DIS), al fine di assicurare una risposta coordinata rispetto al verificarsi di eventi rilevanti in accordo con le strutture dei ministeri competenti in materia[146].

A fronte di tale panorama normativo, la recente Legge 109/2021, di conversione del D.L. 82/2021, istituendo l'Agenzia nazionale e ripartendo puntualmente le

[143] Si tratta del Decreto del Presidente del Consiglio 24 gennaio 2013, Direttiva recante indirizzi per protezione cibernetica e la sicurezza informatica nazionale, pubblicato nella G.U. 19 marzo 2013, n. 66.

[144] Si tratta del QSN, elaborato dal Tavolo Tecnico *Cyber* (TTC) –che opera presso il DIS ed al quale partecipano i rappresentanti *cyber* del CISR (Affari esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo economico), dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica.

[145] Del 2015 sono anche i due d.p.c.m. emanati il 6 novembre in tema di disciplina della firma digitale dei documenti classificati (il n. 4/2015, recante "Disciplina della firma digitale dei documenti classificati e di tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" ed il n. 5/2015, recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva").

[146] D.p.c.m. 17 febbraio 2017.

ISSN 2036-7821

competenze tra specifici soggetti istituzionali, sembra avere finalmente conferito la giusta attenzione alla necessità di garantire anche i diritti fondamentali degli individui in materia di sicurezza informatica; essa consente la realizzazione di una struttura leggera, centralizzata e multidisciplinare, in parte governativa, in parte privata e in parte legata al mondo della ricerca, in grado di far fronte ad una serie di servizi e attività di ricerca, ma anche di rivestire un ruolo primario nelle linee attuative del processo dinamico di implementazione del Piano Strategico Nazionale di Sicurezza Cibernetica, insieme alle altre componenti del sistema governativo nazionale - obiettivo, questo, atteso da tempo.
Essa, insomma, giunge non solo a dare forza agli obiettivi contenuti nel PNRR - che, in merito, vuole dare un impulso decisivo al rilancio della competitività, investendo, con ampi settori di intervento, in primo luogo sulla digitalizzazione e modernizzazione della Pubblica Amministrazione - ma anche ad attribuire, all'interno del nostro ordinamento, le competenze a soggetti specifici, sì che il ruolo del nostro Paese possa essere concreto e consapevole nel perseguimento di obiettivi non frammentari e ben definiti.
Tutto ciò può contribuire a rinforzare l'impianto giuridico e la funzione politica della strategia nazionale sulla *cybersecurity*. Del resto, solo attraverso fondamenta normative solide si può garantire la resilienza della complessa infrastruttura giuridica che, pur esistendo già, deve ancora, in parte, essere sviluppata.

11. Considerazioni conclusive.
Al netto delle novità legislative alle quali si è appena fatto riferimento e che sono ancora troppo recenti perché si possa trarre un bilancio concreto sulla loro efficacia, dalla disamina condotta in tale scritto emergono due conclusioni che appaiono in contraddizione tra loro: da un lato si tende ad un elevato processo di digitalizzazione che, estesosi, ormai, a tutti i settori della vita, sia pubblica che privata, ha consentito progresso e miglioramento; dall'altro si deve provvedere a difendersi da questa stessa estensione, perché da essa deriva un altrettanto elevato rischio di aggressione e compromissione dei dati e delle informazioni personali, con conseguenze anche gravi e che si riflettono sui diritti inviolabili degli individui. Infatti, la trasposizione della vita reale nel mondo virtuale rende particolarmente facile incorrere, nel *web*, in varie tipologie di reati che, però, denotano un'aggravante rispetto a quelle che si verificano nella vita reale, e cioè che nel mondo virtuale sono virtuali anche le identità che in esso agiscono e, quindi, le condotte criminose realizzabili sono molteplici ed anche più difficili da individuare e perseguire in maniera adeguata.
Queste difficoltà, purtroppo, come si è avuto modo di evidenziare, non riguardano specificamente solo il singolo utente, ma si estendono anche alle aziende private ed alle Pubbliche Amministrazioni perché le minacce, data la velocità con cui si diffondono, riescono a colpire ogni settore e realtà della vita quotidiana.

ISSN 2036-7821

Anche la Pubblica Amministrazione, quindi, può diventare vittima di attacchi come quello del *phishing* che, per questi motivi, possono essere considerati l'altra faccia della medaglia, o meglio, il "risvolto" negativo di quella stessa innovazione ed evoluzione tecnologica che, negli ultimi venti anni in particolare, hanno procurato vantaggi che non sono equiparabili neanche a quelli dell'epoca della rivoluzione industriale.

Non è possibile rinunciare alle semplificazioni che il sistema della rete offre. Esse hanno cambiato completamente il mercato, che ora consente opportunità che lo rendono un luogo irresistibile per la varietà di offerta facilmente raggiungibile da chiunque, semplicemente navigando in rete. Ma questi stessi dati, immessi in rete per fruire dei vantaggi che il mercato offre, diventano, purtroppo, un obiettivo per i criminali informatici che riescono ad utilizzarli e ad impossessarsene con la complicità inconsapevole degli stessi utenti che, accettando le condizioni del servizio cui hanno avuto accesso, ne consentono la raccolta per fini non leciti[147].

Insomma, al dinamismo e alla facilità di accesso da parte di chiunque al mercato - e, dunque, all'informazione e alla conoscenza, a prescindere dal luogo, dalla qualifica o dall'esperienza che si possiedano – corrisponde una estrema vulnerabilità proprio del trattamento dei dati inseriti all'interno del sistema[148]. Tutti i rapporti e le ricerche condotte da organismi nazionali ed internazionali sul c.d. "furto di identità" hanno incluso i *phishing attacks* fra le principali tecniche utilizzabili per realizzare una "frode identitaria"[149] perché riescono a carpire informazioni personali, abitudini e stili di vita grazie anche ad operazioni semplici ed usuali, come gli acquisti *on line*[150].

Questi attacchi sono cresciuti in maniera esponenziale negli ultimi due anni (complice anche la situazione pandemica) e ad essi fanno, di solito, seguito ingenti richieste di riscatto di notevole entità inviate non solo alle Pubbliche Amministrazioni, ma anche a grandi società ed alle aziende[151], tutte disposte pure a pagare, sia per ripristinare i sistemi sia perché costrette dalla minaccia di rendere

---

[147] Cfr. M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, su www.federalismi.it, n. 14/2020, pp. 209-234.

[148] Per approfondire il tema si consiglia M. KRANZBERG, *The Information Age: Evolution or Revolution?*, in B. R. GUILE (ed.), *Information Technologies and Social Transformation*, Washington, D. C., 1985, 50 ss.

[149] Dai risultati del *Threat Landscape Report* che l'agenzia ENISA (Agenzia dell'Unione europea per la *cyber*sicurezza) pubblica annualmente per contribuire allo sviluppo di una maggiore sicurezza delle reti e delle informazioni nell'ambito dell'Unione Europea, il *phishing* vanta il primato di rientrare tra le prime 15 *cyber* minacce. L'Agenzia evidenzia che gli attacchi di *phishing* hanno lo scopo di «*…persuade potential victims into divulging sensitive information such as credentials, or bank and credit card details*», ma hanno anche la capacità di centrare l'obiettivo proprio per la facilità con cui vengono divulgate informazioni e dati personali i quali, dunque, necessitano di un sistema di *cyber* sicurezza adeguato, in grado di offrire una protezione capace di preservarne la riservatezza (o confidenzialità), l'integrità e la disponibilità in un tempo dato.

[150] Infatti, il primo alleato degli *hacker* è proprio l'*e-commerce* che, dal 2015, ha prodotto in Italia una crescita più che raddoppiata sull'anno precedente, facendo raggiungere al fatturato italiano vette molto elevate.

[151] BANCA D'ITALIA, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass*, Gruppo di coordinamento sulla sicurezza cibernetica (GCSC), 2018.

pubbliche le informazioni sottratte, da cui potrebbero derivare danni gravi al *brand* ed alla reputazione, oltre al pericolo che si possa venire a conoscenza di informazioni riservate[152].

Chi pone in essere un attacco informatico, dunque, riesce a trovarsi quasi sempre in una posizione di vantaggio rispetto alla sua vittima che, al contrario, si trova in una situazione di soggezione proprio a causa dell'importanza e della rilevanza degli interessi che la condotta criminale potenzialmente o concretamente punta a ledere, e gli strumenti di difesa attualmente a disposizione non sembrano, purtroppo, essere ancora completamente efficienti.

Tale aspetto, insieme con la diffusione sempre maggiore di tale fenomeno, è la tangibile dimostrazione che il settore informatico necessita di una tutela *ad hoc,* più puntuale e prettamente indirizzata a porre rimedio a problemi che denotano un ritardo che, negli anni, si è fatto sempre più evidente e che dipendono da reati che, dato il contesto in cui maturano – e cioè il *cyberspace* - sono troppo specifici per essere tutelati da norme che si adattino ad essi ma che, tuttavia, non li disciplinino direttamente perché nascono riferite a contesti diversi.

La evidenziata assenza ha fatto sì che fosse la giurisprudenza a dovere svolgere un ruolo determinante in merito alla individuazione di tali tipologie di reati, tant'è che, già dodici anni fa, essa aveva affrontato le questioni di fatto e di diritto relativamente all'utilizzo di dati fraudolentemente acquisiti (*user names* e *password*) per ottenere indebiti profitti e per acquistare carte prepagate delle istituzioni coinvolte che successivamente sono state utilizzate sia per la realizzazione di illeciti, sia per aprire conti correnti per il medesimo scopo, sia, infine, per far circolare i profitti dei reati posti in essere[153].

Senza dubbio il ruolo svolto dai giudici è stato fondamentale e determinante, ma non è possibile continuare a credere che le lacune possano essere colmate solo dall'opera dell'interprete del singolo caso di specie.

---

[152] Da un anno a questa parte gli attacchi hanno utilizzato l'emergenza da Coronavirus come esca per attirare vittime, in particolare, sfruttando l'attesa e la speranza relative al vaccino contro il *virus*; per cui è accaduto di frequente che l'utente meno attento abbia cliccato sulla *mail* convinto di accedere a notizie di speranza a lui direttamente indirizzate, ed invece abbia installato *file* malevoli sul proprio dispositivo. Non solo. Gli attacchi sono stati mirati oltre che nei confronti di ospedali, contro la stessa OMS (Organizzazione Mondiale della Sanità) che, come l'INPS, nel primo semestre del 2020, ha avuto dei problemi informatici, per fortuna in parte arginati.

[153] Si fa riferimento, specificamente, alla sentenza del Tribunale di Milano (Giudice per le indagini preliminari) del 10 dicembre 2007 n. 888, nella quale è stato sostenuto che «*Sono penalmente responsabili coloro che, associandosi ed avvalendosi delle tecniche di* phishing*, realizzano furti di identità e truffe aggravate attraverso accessi abusivi a sistemi di* home banking *ai fini di utilizzare indebitamente carte di credito e di pagamento. Il reato è da considerarsi transnazionale ai sensi dell'art. 3, co. 1, lett. b, l. 16 marzo 2006, n. 146, dal momento che trattasi di illeciti commessi in Italia ma aventi una parte sostanziale di preparazione e pianificazione in Romania*». In tale sentenza, il giudice aveva affermato la sussistenza di un vincolo associativo continuativo allo scopo di commettere una serie di delitti, ritenendo, dunque, applicabili, al fenomeno "*phishing*" gli artt. 615 *ter* c. p., 617 *sexies* c. p., 640 c. p. e l'art. 12 della L. 5 luglio 1991, n. 197.

ISSN 2036-7821

Dunque, servono norme più puntuali per la definizione delle specifiche tipologie di reato, ma servono anche l'attuazione di un'azione congiunta ed investimenti più proficui sugli strumenti di prevenzione, tutela ed alfabetizzazione, sì da conseguire un maggiore livello di responsabilizzazione al quale devono essere chiamati tutti, dagli utenti individuali della rete alle istituzioni pubbliche, in modo che ciascuno possa, nella consapevolezza delle proprie possibilità e dei propri limiti - oltre che, ovviamente, delle proprie funzioni - contribuire alla tutela di un ambiente - quello digitale - ancora troppo sconosciuto, non per questo ignorato, ma, spesso, utilizzato con assoluta superficialità.

Attraverso il Reg.(UE) 2019/881 l'Unione europea ha dimostrato di volere lasciare totalmente alla competenza degli Stati membri l'apparato sanzionatorio della *cyber*sicurezza; dal canto suo, il Legislatore italiano, con il D.L. n. 105 del 2019, ha delineato un modello delle competenze interne all'amministrazione italiana, ma pur avendo dato vita ad un bilanciamento tra le attività dei diversi ministeri, comitati e agenzie - puntando a mantenere il più possibile invariati gli oneri per il bilancio dello Stato – non è riuscito, però, a dipanare effettivamente e concretamente le competenze in un settore così strategico come quello della *cybersecurity*.

Insomma, quella frammentarietà che era già stata evidenziata, nel nostro ordinamento, dalle Direttive della Presidenza del Consiglio dei Ministri del 2013 e del 2015, non è stata superata e non si è ancora giunti a quel modello del "coordinamento", auspicato come il più coerente con la dimensione e la velocità d'azione del fenomeno *cyber*sicurezza che, a questo punto, ci si attende che possa essere conseguito grazie ai recenti interventi normativi.

Infatti, il Regolamento (UE) 2021/887 denota che l'Unione abbia compreso la necessità di un approccio strategico di tipo globale, fondato sulla cooperazione internazionale e sulla condivisione di informazioni a tutti i livelli, redistribuendo responsabilità tra settore pubblico e privato, al fine di creare un clima di fiducia reciproca che favorisca, nel pubblico interesse, il requisito della solidità dei sistemi.

Nella consapevolezza, dunque, che la *cybersecurity* debba essere una responsabilità condivisa, l'auspicio è che, da un lato attraverso il rafforzamento delle forme di collaborazione pubblico-privato nella combinazione di modelli differenti, necessariamente integrati, ma con una regia unitaria; e dall'altro attraverso l'attività della neo istituita Agenzia nazionale sulla tutela della sicurezza informatica - in uno con la puntuale attribuzione delle competenze – si possa effettivamente riuscire a superare la frammentarietà e la scarsa adeguatezza di risultati che attualmente ancora si registrano, a vantaggio di un consolidamento del sistema delle comunicazioni nel suo complesso, all'interno del quale anche i cittadini dovranno essere responsabilmente consapevoli, nell'interesse proprio quanto di quello generale.

ISSN 2036-7821