CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

CONTRAFFAZIONE DELLA FIRMA DIGITALE: IL CASO GREEN PASS

In linea con un mondo che continua ad essere sempre più interconnesso e dipendente dall'efficace funzionamento e dalla resilienza di reti, sistemi e dispositivi informatici – che conferiscono natura ubiquitaria ai contenuti da essi trasportati, elaborati e conservati – l'architettura nazionale ha conosciuto, nel biennio della pandemia, interventi di modifica miranti a razionalizzare e snellire le capacità operazionali del sistema - Paese nel nuovo mercato economico digitale.

di **Giulia Guastella**
IUS/01 - DIRITTO PRIVATO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Giovedì 3 Marzo 2022

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

In line with a world that continues to be increasingly interconnected and dependent on the effective functioning and resilience of networks, systems and IT devices - which confer ubiquitous nature to the contents they transport, processed and stored - national architecture has known, in the two-year period of the pandemic, modifications aimed at rationalizing and streamlining the operational capabilities of the country - system in the new digital economic market.

Sommario: 1. Premessa; 2. Il documento informatico: nozione e profili giuridicamente rilevanti; 3. Primo vizio: patologia della titolarità di firma; 4. Secondo vizio: patologia della circolazione della chiave di firma; 5. Focus su un caso concreto di contraffazione: Il caso Green Pass; 6. Attacco alle chiavi private: Il fenomeno Man in The Middle; 7. Conclusioni.

1. Premessa

La questione dibattuta intorno al fenomeno della contraffazione della firma digitale è ben complessa e conosce la sua maggiore diffusione negli anni che sono stati investiti dall'emergenza sanitaria globale da COVID -19, ove la neofita fattispecie del commercio elettronico dai contenuti digitali ha favorito lo sviluppo di modalità di consumo dematerializzate e la conseguente emersione di un nuovo soggetto attivo nei mercati virtuali: il consumatore telematico.

Col sopraggiungere di un fenomeno fortemente impattante a livello planetario, quale era la pandemia da Coronavirus, era verosimile che un cambiamento si producesse non solo sull'esistenza umana stricto sensu, ma anche, e più incisivamente, sull'andamento dell'economia.

Sono stati i mercati digitali a beneficiarne in maggior misura, uscendone straordinariamente rafforzati dai prolungati e reiterati lockdown[1] sanitari: i grandi digital player[2] globali hanno raggiunto posizioni di forza economica, informativa e regolatoria oltre ogni immaginazione.

La globalizzazione del diritto trova compimento nella nuova dimensione immateriale e delocalizzata, senza frontiere, generata dalle piattaforme commerciali digitali veicolate tramite le reti di comunicazione elettronica. Si registra a tal proposito la nascita di un nuovo settore interdisciplinare del diritto che risponde pienamente alle istanze regolatorie

CamminoDiritto.it
ISSN 2421-7123

di tale complesso fenomeno, noto come High Tech Law[3], o Diritto privato delle nuove tecnologie.

2. Il documento informatico: nozione e profili giuridicamente rilevanti

Questa breve premessa risulta necessaria al fine di introdurre l'oggetto della presente analisi che, da questo momento in poi, si concentrerà sull'emersione del nuovo e ormai sempre più diffuso tipo di scrittura privata, ovvero quella elettronica, con un'attenzione che impone di distinguere fra le varie tipologie di documento informatico.

Seguendo una prima prospettiva classificatoria, il contratto virtuale costituisce una sottospecie dei contratti a conclusione telematica – ossia quei contratti stipulati mediante l'utilizzo delle nuove tecnologie informatiche e telematiche di comunicazione.

Si devono, a questo punto, precisare meglio i limiti dell'area definitoria "contratto virtuale" operando una classificazione tra "contratto virtuale in senso ampio" e "contratto virtuale in senso stretto".

Il contratto virtuale in senso ampio può essere definito con riferimento alla sottospecie di contratto telematico in senso stretto concluso utilizzando la tecnologia e-mail[4] o mediante altri dispositivi telematici similari - basati su servizi Internet - di mera trasmissione del messaggio a contenuto negoziale.

Il contratto virtuale in senso stretto può essere definito con riferimento allo specifico contratto - sottospecie di contratto telematico - concluso utilizzando lo specifico servizio world wide web[5] di Internet - come assetto materiale tecnologico, mezzo di offerta in incertam personam, predisposto unilateralmente dall'offerente - mediante pressione del cd. "tasto negoziale virtuale".

Il contratto virtuale in senso stretto, oltretutto, è caratterizzato dall'assenza di trattative tra le parti, dalla predisposizione unilaterale e dall'offerta al pubblico indistinto: è, pertanto, qualificabile come contratto d'impresa in serie, predisposto e asimmetrico. A questo proposito, viene in mente l'ulteriore caratteristica del contratto virtuale - comune ai contratti di massa in generale - sintetizzata nella tendenziale indifferenza rispetto all'identità dell'oblato: tendenziale perché tale considerazione si ritiene essere applicabile principalmente ai contratti virtuali conclusi mediante comportamento concludente ex art. 1327 c.c., che non esaurisce la fenomenologia dei contratti virtuali in senso stretto.

Per ciò che concerne i profili squisitamente formali, il contratto virtuale in generale è

CamminoDiritto.it
ISSN 2421-7123

caratterizzato dall'utilizzo - per sua formazione e conclusione - della forma informatica, anche detta elettronica, resa disponibile dal substrato tecnologico dello spazio virtuale: è irrilevante che l'accordo telematico si raggiunga tramite scambio di e-mail, mediante accesso al sito web di riferimento o altro mezzo di comunicazione digitale.

La forma utilizzata per il perfezionamento di questa nuova, e grandemente avveniristica, tipologia di contratto, è detta infatti atipica, in contrapposizione alle forme informatiche notoriamente tipizzate dall'ordinamento giuridico.

Non sorprende, peraltro, rilevare come la diffusione e affermazione della forma elettronica atipica - basata su documenti informatici privi di sottoscrizione - si inserisca a pieno titolo nel più ampio fenomeno della crisi della sottoscrizione e del predominio del testo grafico: integra il cd. aformalismo negoziale dei rapporti economici di business che si contrappone al più rigido formalismo del Codice civile relativamente ai negozi sorti su beni immobili.

In subordine, occorre precisare che il riconoscimento della rilevanza giuridica del documento informatico ha introdotto almeno quattro rischi, dei quali uno è di natura soggettiva, ed i restanti sono di tipo oggettivo.

In primo luogo, viene in rilievo il rischio relativo all'identificazione del soggetto. Seguono, ma non in ordine di importanza, i pericoli che riguardano l'incertezza del contenuto, l'indeterminatezza del tempo della stipulazione e l'indeterminatezza del luogo ove viene concluso il contratto digitale.

In via preliminare va rilevato, con riferimento ai contenuti del documento informatico, che essi sono riproducibili all'infinito. Tale postulato si può declinare nel senso in cui la rappresentazione informatica di una firma chirografa non può suscitare alcun affidamento, in quanto può essere facilmente riprodotta ed associata a contenuti diversi rispetto a quelli a cui era in origine destinata; un'osservazione che è di primo piano per proseguire con la presente analisi e che vuol sottolineare come gli strumenti di autentificazione di un documento informatico non possono consistere in una mera riduzione in forma elettronica dei metodi usualmente impiegati nell'autentificazione di una scrittura privata tradizionale.

Problemi specifici si pongono, poi, con riguardo al profilo della genuinità dei contenuti.

Venendo al problema dell'indeterminatezza del luogo di stipula, una prima osservazione concerne il fatto che alcuni supporti notoriamente impiegati per la documentazione informatica, ad esempio i compact disk[6] riscrivibili, o le pen drive[7], possono essere

CamminoDiritto.it
ISSN 2421-7123

alterati senza che resti traccia della manipolazione effettuata[8].

Per ovviare a tali inconvenienti, sono state predisposte delle barriere logiche che consentono di limitare l'accesso alla creazione e alla modificazione del contenuto dei documenti informatici.

Una tecnica efficace per garantire la provenienza e la genuinità di una rappresentazione informatica, consiste nella predisposizione di uno sbarramento logico alla generazione e alla modificazione del contenuto. Tale sbarramento può essere costituito cifrando il testo destinato alla formulazione della dichiarazione in base ad un criterio noto al solo emittente[9].

Il metodo consiste nell'impiego di una chiave nota ad un solo soggetto che viene considerato l'unico titolare della firma generata: da quel momento in avanti, solo la chiave di cifratura può determinare il contenuto del documento.

Questo primo espediente costituisce, per certo, un metodo di autentificazione della provenienza e di attestazione della genuinità dei contenuti. La sua efficienza dipende, infatti, da alcuni fattori imprescindibili: primo fra tutti, la garanzia che le chiavi di attivazione dell'algoritmo di firma sono attribuite al soggetto che essa indica, andando a circoscrivere la cd. "paternità". A ciò, segue la garanzia che le stesse restino nella disponibilità esclusiva di quel soggetto. Infine, si sottolinea la robustezza del sistema di cifratura impiegato.

È innegabile che tra il caso più rischioso dei documenti informatici riscrivibili privi di protezione e quello considerato più sicuro dei documenti muniti di firme elettroniche qualificate, esiste una gamma di situazioni intermedie.

In relazione a tali situazioni, il Legislatore ha disposto all'art. 10, secondo comma, del t.u.d.a., che è rimessa ad un discrezionale apprezzamento, da compiere con riferimento al caso concreto, la valutazione circa la sicurezza ed affidabilità dei metodi impiegati.

Si vuole a tal fine precisare come i rischi di falso documentale relativo alla provenienza di un documento informatico firmato, possono essere ricondotti a due classi fondamentali di patologie.

3. Primo vizio: la patologia della titolarità di firma

CamminoDiritto.it
ISSN 2421-7123

La prima anomalia è da ricondurre alla cd. patologia della titolarità della firma, che si verifica quando l'intitolazione della chiave è viziata.

Tale situazione si manifesta in due ipotesi: quando il vizio è genetico (errore del certificatore, falsa attestazione dell'identità del titolare), e quando il vizio è funzionale (attribuzione della chiave di firma già assegnata ad altri, smarrimento del dispositivo di firma).

Il fenomeno richiede, tuttavia, di essere introdotto da un distinguo che risulta preliminare all'individuazione prima, ed alla risoluzione poi, di questo specifico problema, ed attiene alle peculiari nozioni di "firma digitale" e di "chiave di firma".

Mentre la prima è un valore simbolico, espresso in bit[10], che dichiara e documenta l'adesione di un soggetto ad un testo, indicandone la precisa identità, la seconda è un valore algebrico anch'esso espresso in bit, che invece connota in concreto le modalità di cifratura, rendendo diverso da ogni altro il risultato di quelle operazioni.

La "chiave" delle firme digitali è quindi il valore che consente la generazione (mediante la "chiave privata") o la verifica (mediante la "chiave pubblica") di una sottoscrizione, di una certificazione o di una marcatura temporale.

4. Secondo vizio: la patologia della circolazione della chiave di firma

La seconda categoria del problema in esame fa riferimento, invece, alla patologia della circolazione della chiave di firma, che si verifica ogni qualvolta avviene un uso non autorizzato della stessa.

Più specificamente, viene compromessa l'esclusività sull'impiego di chiavi di firma validamente attribuite.

Passando in rassegna qualche ipotesi, ciò può avvenire a causa dell'installazione di software[11] destinati ad attivarsi in occasione dell'impiego di un dispositivo personale per la creazione di una firma. In tale occasione, i programmi sfruttano i dati utilizzati per generare la firma voluta dal suo titolare per apporre la stessa contemporaneamente anche ad altri file, senza che egli lo sappia.

I software possono essere installati sia all'insaputa o contro la volontà dell'utente del dispositivo di firma, sia contro quella del titolare del sistema hardware[12] al quale il

CamminoDiritto.it
ISSN 2421-7123

dispositivo viene applicato (in tal caso si tratta dell'intrusione di virus informatici).

La loro presenza può non essere rilevata dall'utente della macchina e il loro impiego per la creazione di documenti contraffatti non lascia traccia sugli stessi.

Nei paragrafi che seguono, si vogliono considerare alcune ipotesi di falso – lungi dalla pretesa di esaurire tutte le fattispecie possibili – col modesto intento di offrire un campione utile alla prospettazione di alcune soluzioni – come si auspica – ai problemi che possono porsi nella pratica.

Posto che vi sono alcune patologie che possono verificarsi sia al momento della certificazione di una coppia di chiavi simmetriche (quelle che abbiamo già inquadrato come "patologie della titolarità"), sia al momento della loro intitolazione (le "patologie dell'intitolazione", per l'appunto), per tale ragione non si può escludere a priori che anche la dichiarazione sottoscritta con firma digitale venga resa sotto falso nome o sotto nome altrui o, in ogni caso, da un soggetto diverso da colui che risulta essere titolare della firma [13].

Sebbene sia uno fra quelli in cui è meno auspicabile imbattersi, si tratta di uno dei fenomeni di contraffazione più diffusi: in particolari situazioni, può accadere che, al momento della certificazione della chiave pubblica, la stessa sia compiuta indicando un nome immaginario o il nome altrui. In questo modo, non solo il documento informatico sottoscritto con la chiave privata di quella coppia potrebbe essere imputato ad una persona inesistente, ma potrebbe anche accadere che venga imputato ad una persona esistente e tuttavia diversa da colui che utilizza quella firma digitale. Quello appena citato è, certamente, un caso paradigmatico di patologia genetica della titolarità.

Per scongiurare questo pericolo, il regolamento fa obbligo al certificatore di "identificare con certezza la persona che fa richiesta della certificazione"[14].

Se, infatti, il certificatore indica falsamente l'identità del titolare di una firma, poco importa se a motivo di dolo o di colpa, è tenuto obbligatoriamente a risarcire il danno che ne consegue a titolo di responsabilità extracontrattuale, se il danneggiato è un terzo che sia stato indotto a fare affidamento sulla falsa attestazione compiuta dal certificatore, oppure a titolo di responsabilità contrattuale, se il danneggiato è il titolare stesso che non abbia potuto conseguire gli effetti della dichiarazione compiuta in forma elettronica a causa dell'erronea attribuzione della sottoscrizione.

Infatti, per un corretto svolgimento dell'operazione, è necessario non solo che il titolare

CamminoDiritto.it
ISSN 2421-7123

della chiave pubblica sia colui che effettivamente la diffonde come propria, ma anche che questo soggetto possa fare affidamento in ogni momento sulla corretta certificazione dell'attribuzione della propria firma.

Giova ricordare, a questo proposito, che la legge penale non muta né la specie né tantomeno il quantum di pena da irrogare in relazione al campo di applicazione – virtuale o non virtuale - in cui è chiamata a produrre i suoi effetti e pertanto, sia che si tratti di firme tradizionali, sia che si tratti di firme elettroniche qualificate, se l'imputazione della regiudicanda è la falsità in atti o la certificazione in nome altrui, s'intende comunque integrato il reato di "sostituzione di persona", disciplinato all'art. 494 del c.p.

Si tratta, peraltro, di un tipo di illecito che nei più recenti anni, caratterizzati dall'avvento delle tecnologie informatiche e telematiche, ha assunto una consistenza ed una diffusione tali da suscitare un permanente allarme sociale tra la popolazione civile. I mezzi di cui la criminalità del web si serve per compiere i propri traffici illeciti sono i più comuni, e fra questi vi è proprio l'utilizzo della posta elettronica.

La giurisprudenza di legittimità è unanime nel ritenere che integra il reato di sostituzione di persona (art. 494 c.p.), la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete Internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità[15].

Si vuole ora accennare ad una delle più conclamate patologie della circolazione della chiave di firma, che ha luogo allorché si fa un uso negativo e disfunzionale della crittoanalisi[16].

In taluni e particolari casi, infatti, la crittoanalisi consiste nell'attività orientata a forzare un sistema per conoscere la chiave privata da utilizzare per scopi illeciti, ad esempio per la generazione della firma altrui.

Analizzando il contenuto di un testo cifrato attraverso particolari tecniche statistico – matematiche, si possono ottenere essenziali informazioni sul testo in chiaro. Per fortuna, svolgere questa operazione non è sempre possibile, in quanto la maggior parte dei cifrari moderni è ancora al sicuro perfino dalla minaccia delle più sofisticate tecniche di crittoanalisi.

Per comprendere il senso di tale pericolo, può tornare utile svolgere un ragionamento

CamminoDiritto.it
ISSN 2421-7123

simile a quello compiuto per la generazione di una firma digitale. Come si è già detto, l'attività connessa alla tipologia di firma cosiddetta "digitale" non si declina in un mero sottoscrivere, bensì in un cifrare, motivo per cui tendenzialmente si parla di "crittografia", prim'ancora che di crittoanalisi.

In particolare, il valore che esprime il contenuto di un documento o una sua rappresentazione sintetica, detta "impronta[17]", può essere sottoposto ad un trattamento informatico tramite un procedimento che impiega una chiave (la chiave privata, per definizione) per ottenere un contenuto cifrato (la firma).

Applicando lo stesso procedimento alla firma, ma questa volta con la chiave pubblica, si può ottenere come risultato il messaggio di partenza[18].

Gli algoritmi attualmente riconosciuti dal DPCM 8 febbraio 1999 per la generazione e la verifica delle firme digitali sono solo due e sono noti (art. 2): l'algoritmo R.S.A. (o "Rivest – Shamir – Adlemn Algorythm[19]") e l'algoritmo D.S.A. (o "Digital Signature Algorithm[20]").

Quando si fa riferimento ad un algoritmo crittografico, è fondamentale poter riscontrare la presenza di quattro caratteri:

Autenticazione: processo tramite il quale si attesta l'identità di ciascun partecipante ad una comunicazione; Segretezza: è essenziale che nessuno possa leggere un messaggio, fatta eccezione per il destinatario desiderato; Integrità: si riassume nella protezione da modifiche non autorizzate operate sul messaggio trasmesso (il materiale inviato al destinatario non deve, cioè, poter essere alterato prima della consegna); Non ripudio: si tratta di un meccanismo atto a fornire la certezza che chi trasmette un messaggio non possa negare di averlo inviato. La chiave pubblica e la chiave privata sono due valori tra loro legati da algoritmi noti, ma che, utilizzando i principi dell'aritmetica modulare[21], non consentono di risalire dall'uno all'altro attraverso sistemi matematici diretti, ma solo per tentativi. Ecco spiegato il motivo per cui non sempre si può assicurare la buona riuscita della crittoanalisi su un messaggio privato.

Si è parlato di una sorta d'invulnerabilità del sistema di cifratura a chiavi simmetriche, perché, allo stato delle tecniche note, il crittoanalista non può fare altro che procedere per tentativi, i quali, in base a valutazioni di carattere statistico, per forzare una coppia di chiavi asimmetriche di robustezza media tendono ad essere miliardi di miliardi[22].

Nondimeno, da una parte, non si può escludere la possibilità teorica che il tentativo di

CamminoDiritto.it
ISSN 2421-7123

crittoanalisi riesca in tempi tali da consentire la forzatura del sistema prima che la chiave sia scaduta di validità; dall'altra, anche se per il momento non si conosce un sistema per forzare una coppia di chiavi asimmetriche, non esiste una dimostrazione teorica che escluda la possibilità di elaborare un simile sistema.

Il metodo delle firme digitali, pertanto, si può ritenere affidabile solo in considerazione dello stato attuale delle tecniche di crittoanalisi, e cioè solo se non verrà elaborato un modello matematico che consenta di risalire dalla firma alla chiave privata impiegata per generarla. In teoria, dunque, la crittoanalisi potrebbe anche avere successo. In tal caso, dalla conoscenza della chiave pubblica e dalla notorietà dell'algoritmo utilizzato per creare la coppia di chiavi asimmetriche, si potrebbe ricavare il valore della chiave privata.

Più tempo passa, più tentativi si possono compiere, più aumenta la possibilità di riuscire nella ricostruzione della parte segreta della coppia di chiavi[23]. Proprio per questo, il regolamento stabilisce che la chiave pubblica (e, con essa, l'intera coppia di chiavi), ha un periodo di validità limitato nel tempo. L'obiettivo è quello di massimizzare la protezione.

L'art. 22, lett. f, t.u.d.a., che escludeva che le chiavi potessero avere un periodo di validità superiore a tre anni, è stato abrogato dall'art. 8 d.P.R. n. 137/02.

Esse, infatti, per la loro sopravvenuta riproducibilità, non potrebbero più essere considerate come strumento di autentificazione informatica ai sensi dell'art. 1, lett.cc, t.u.d.a. e, dunque, non sarebbero più riconducibili alla definizione normativa di firma elettronica.

Si vogliono citare, a titolo di esempio, alcune fra le più note e affinate tecniche di crittoanalisi attuabili mediante le combinazioni possibili del cifrario:

Brute-force[24]: avviene tramite il calcolo di tutte le possibili combinazioni di chiavi del cifrario. Con l'aumento della potenza di calcolo degli elaboratori questa tecnica sta diventando sempre più efficace; basti pensare al Cracking[25] del DES a 56 bit[26] con un computer multiprocessore costruito dall'EFF in grado di violare l'algoritmo in meno di tre giorni di calcolo. Crittoanalisi differenziale: avviene tramite l'analisi delle distanze numeriche dei caratteri presenti nel testo cifrato e l'ausilio di sofisticate tecniche matematiche unite ad algoritmi sempre più veloci. Man-In-The-Middle[27]: sfruttando il sistema delle infrastrutture PKI[28], un eventuale intruso può posizionarsi tra un mittente ed un destinatario e scambiare le loro chiavi pubbliche e private con altre opportunamente modificate. Dalla presente analisi è possibile evincere che le tecniche di crittoanalisi diventano sempre più sofisticate grazie all'aumento della potenza di calcolo dei computer; tuttavia, solo con la condivisione delle informazioni e delle tecniche degli algoritmi

CamminoDiritto.it
ISSN 2421-7123

crittografici si può ottenere maggiore controllo. Per questo ed altri motivi di carattere logistico, la filosofia open source[29] è divenuta strumento di vitale importanza per il settore crittografico: gli algoritmi crittografici più importanti ed utilizzati da tutti devono necessariamente essere di pubblico dominio, in quanto, ad oggi, è quasi impensabile potersi fidarsi delle "black box"[30].

Ciò nonostante, è inevitabile un risvolto negativo della medaglia: l'evoluzione della rete e l'aumento di processori connessi alla rete Internet, ci dimostrano quanto, in ogni caso, la prevenzione e la sicurezza siano ancora gli ultimi, fidati, approdi di un'informazione basata sulla trasparenza.

5. Focus su un caso concreto di contraffazione: Il caso Green Pass

In Italia, a seguito della diffusione della pandemia da Covid – 19 avvenuta all'inizio del 2020, è stata introdotto il possesso della certificazione verde, indicata comunemente con l'espressione "Green Pass[31]", come documento con effetti di pubblicità per coloro che si fossero vaccinati con la prima dose di mRNA[32]; il possesso del certificato, inizialmente facoltativo e richiesto in extrema ratio per partecipare a talune attività di carattere pubblico come cerimonie civili e religiose, nonché per accedere a residenze sanitarie assistenziali, spostarsi in entrata e in uscita da territori classificati come "zona rossa" o "zona arancione", dal 6 agosto 2021 è divenuto ufficialmente obbligatorio per accedere a tutti i servizi e le attività, nei luoghi chiusi e destinati al pubblico[33].

Successivamente, dal 1° settembre 2021, l'obbligo di esibizione, insieme all'obbligo di indossare la mascherina FPP2[34], è stato esteso anche al personale scolastico e universitario e agli studenti, nonché a chi utilizza alcuni mezzi di trasporto[35].[13]

Sul versante amministrativo, e salvo che il fatto non costituisca più grave reato - nei confronti del quale è prevista la pena detentiva – per chi non è provvisto di valida certificazione e acceda comunque nei locali o alle attività in cui è richiesta l'esibizione, la legge prevede che sia elevata una sanzione pecuniaria compresa fra € 400,00 ed € 1000,00.

Queste misure sanzionatorie, previste tassativamente dal Codice ed inserite nei decreti adottati dal Governo come misure d'urgenza per il contenimento della pandemia, dovrebbero produrre almeno due tipi di effetti sulla popolazione civile.

In primo luogo, dovrebbero disincentivare, o almeno scemare grandemente, qualsiasi tendenza alla violazione degli obblighi di legge; in secondo luogo, dovrebbero condurre la

CamminoDiritto.it
ISSN 2421-7123

popolazione a temere una severa repressione da parte delle autorità avverso quelle che si possono definire, a tutti gli effetti, delle condotte antisociali. Tuttavia, i numerosi episodi di contrasto alle disposizioni di legge intercorsi nel biennio appena trascorso, hanno dimostrato esattamente il contrario nella misura in cui hanno dato luogo a diversi episodi di criminalità.

Altra questione - che si colloca in via preliminare a qualsiasi valutazione di merito - riguarda il sistema attraverso la quale la stessa certificazione opera. Prodromica a qualsiasi operazione successiva è, infatti, la funzione svolta dal meccanismo di autenticazione. La certificazione, emessa esclusivamente dalla Piattaforma nazionale del Ministero della Salute a seguito di avvenuta somministrazione del vaccino contro il Covid-19, contiene un codice bidimensionale (cosiddetto "QR Code[36]") che permette di verificarne l'autenticità e la validità attraverso un sistema di crittografia a doppia chiave. Ogni certificazione viene pertanto prodotta digitalmente con una chiave privata dall'Ente che la rilascia (che, in Italia, è il Ministero della Salute).

Le chiavi private, a loro volta, assicurano l'autenticità delle certificazioni, e vengono custodite in sistemi di massima sicurezza. Le corrispondenti chiavi pubbliche vengono poi utilizzate per verificare le certificazioni attraverso le applicazioni di verifica (in Italia è la "VerificaC19[37]"), in possesso delle esclusive amministrazioni delegate dal singolo Stato.

Questo sistema di crittografia, cd. a doppia chiave, assicura che non sia possibile risalire dalla chiave pubblica alla chiave privata e quindi risolve il maggiore problema rendendo impossibile produrre certificazioni non autentiche.

Ciò consente, in primo luogo, di non essere coinvolti in fenomeni di traffici indesiderati – viene in rilievo, a tal proposito, la nota operazione di contraffazione e di vendita diffusa di certificati falsi, fortemente agevolata da una varietà di canali telematici come Telegram, anche nota come "Fake Pass[38]" - sia di non esporsi a quelle che potrebbero essere delle pesanti conseguenze penali che avrebbero luogo all'integrarsi di diverse fattispecie tipizzate: nel caso di esibizione di certificato contraffatto (integrabile la falsità materiale commessa da privato, art. 482 c.p.), uso di certificato falso (integrabile l'uso di atto falso, art. 489 c.p.), esibizione di certificati altrui (integrabile il delitto di sostituzione di persona, art. 494 c.p.).

6. Attacco alle chiavi private: Il fenomeno "Man In The Middle"

Con riguardo al campo della crittografia, che si edifica sul requisito della confidenzialità, tipico della sicurezza informatica, si è accennato all'esistenza del fenomeno "Man in The Middle" ogni volta in cui si presenta il rischio di subire un trafugamento dei propri dati

CamminoDiritto.it
ISSN 2421-7123

sensibili a seguito dell'introduzione di un soggetto esterno tra il mittente e il destinatario di una conversazione telematica.

Ciò può avvenire tra conversazioni instauratesi fra privati, ma anche fra dispositivi aziendali che effettuano tra loro transazioni economiche.

Pertanto, in questa sede, si vuole tentare di approfondire la questione prestando maggiore attenzione alle dinamiche di questa tipologia di attacco, ormai sempre più frequente sui canali della rete Internet, luogo privilegiato per la loro diffusione.

Nella fattispecie ad oggetto, può accadere che in una connessione instauratasi in maniera legittima tra due utenti o due dispositivi, un terzo soggetto si pone illegittimamente "in the middle", cioè nel mezzo, per perseguire i propri scopi illeciti.

L'attacco più diffuso è quello che avviene all'interno di una rete Wi-Fi pubblica non crittografata, come la rete degli aeroporti, dei bar o di altri esercizi commerciali. Tuttavia, diversi sono gli attacchi MITM praticabili, per citarne alcuni: Rogue access point[39], IP spoofing[40], DNS spoofing[41], HTTPS spoofing[42], Sniffing[43].

Occorre premettere che negli ultimi anni, i più esperti produttori di software, uniti agli ingegneri qualificati del settore ICT[44], hanno ottenuto qualche risultato positivo dopo essersi posti l'ambizioso obiettivo di arenare il MITM mediante la realizzazione del protocollo di rete HTTPS[45] che, a differenza del precedente protocollo http, è più sicuro perché crittografato.

Tuttavia, prima di proseguire con l'analisi del suddetto protocollo, una breve digressione va fatta in merito alla nozione di crittografia.

La crittografia permette di effettuare una conversione dei dati da un formato leggibile in un formato codificato il quale, a sua volta, può essere letto solo dopo che è stato decrittato. Pertanto, solamente la persona autorizzata alla lettura può decriptare i dati e accedere alle informazioni nel formato originale.

Tuttavia, dal vasto campo della cyber security apprendiamo che, oltre ai noti sistemi di cifratura a chiave simmetrica ed asimmetrica, esiste un terzo tipo di crittografia, detto end – to – end[46], utilizzato principalmente dalle piattaforme social WhatsApp, Messenger e Telegram.

CamminoDiritto.it
ISSN 2421-7123

La sua peculiarità è insita nel fatto che permette di proteggere la privacy e le comunicazioni mediante l'uso di un doppio paio di chiavi crittografiche necessarie per cifrare e decifrare i messaggi in viaggio da un punto all'altro della comunicazione.

Ogni utente, infatti, utilizzerà una chiave pubblica e una chiave privata, legate tra loro in maniera reciproca. La chiave privata è destinata a rimanere sul dispositivo dei due "comunicanti", e servirà a decrittare i messaggi in arrivo; la chiave pubblica, invece, sarà condivisa con l'interlocutore e sarà utilizzata per crittografare i messaggi in uscita. Questa cifratura permette di rendere innocui tentativi di attacco Man in The Middle, che mirano a trafugare dati e informazioni personali "intercettando" le comunicazioni tra due o più utenti.

Tutto ciò ci permette di compiere alcune riflessioni.

Da un lato, l'evoluzione della tecnologia e l'uso frequente che di essa facciamo, ci impone un'evidente responsabilità nei confronti dei nostri dati sensibili i quali, di fatto, rappresentano una chiara trasposizione dei nostri dati identificativi sul piano virtuale. La valenza di un documento personale cartaceo come la carta d'identità, o il codice fiscale, non ha nulla in più rispetto ad una certificazione digitale che possiede gli stessi contenuti.

Inoltre, la cultura dell'informazione, che ormai si diffonde soprattutto attraverso la rete, ci mostra come la sicurezza informatica si muova necessariamente attraverso due direttrici.

La prima è nel senso di realizzare prima, e promuovere dopo, dei validi sistemi di firewall [47]. Nel far ciò, affida ai senior consultant[48] delle società di consulenza informatica lo sviluppo di nuove soluzioni software per i clienti, sfruttando la confidential computing technology e gli Smart contracts, per creare nuove app che massimizzino la fiducia, promuovano la tutela della privacy e la sicurezza dell'individuo.

La seconda direttrice, seguendo le sorti della prima, attraversa il campo dell'installazione degli aggiornamenti, ne promuove la pubblicità, lavora sulla fidelizzazione degli utenti incentivandoli alla conoscenza delle più sofisticate tecniche di protezione dei propri dispositivi. E questo, di riflesso, rappresenta senz'altro un bene per la comunità degli internauti.

Questa digressione, utile per ricollegarsi alla questione della sicurezza dei protocolli di rete, risulta tanto più imprescindibile laddove si vuol porre in risalto la circostanza tale per cui neanche l'HTTPS, oggi, fornisce una garanzia di sicurezza assoluta, poiché il malintenzionato che si serve del Man in The Middle per accedere ad un dispositivo

CamminoDiritto.it
ISSN 2421-7123

elettronico, può avere ugualmente accesso ad una serie di dati illeggibili.

Queste osservazioni sono fondamentali per comprendere come, non essendo possibile prevenire le mosse dell'offensore in un campo talmente ignoto quale è quello dell'underground criminale, la miglior difesa contro questo tipo di attacchi è la prudenza.

Il vasto settore della sicurezza informatica, per queste ragioni, ha congegnato una serie di accorgimenti e di strumenti adeguati a garantire prudenza.

È necessario, innanzitutto, evitare di connettersi ad hot - spot[49] pubblici poiché spesso si tratta di reti Wi-Fi con misure di sicurezza minime o, nella peggiore delle ipotesi, sprovviste di crittografia.

In secondo luogo, utilizzare una VPN – acronimo per Virtual Private Network[50] -, potrebbe essere una soluzione efficace contro un attacco simile, perché le VPN provvedono ad applicare una propria crittografia a tutto il traffico veicolato. Va da sé che la stessa sicurezza di una VPN è proporzionale alla serietà e all'efficienza del provider che la fornisce.

Per proteggersi invece dagli attacchi MITM basati su malware[51] il requisito più importante è, banalmente, quello di non installare malware; inoltre, occorre monitorare con frequenza il proprio antivirus ed effettuare gli opportuni aggiornamenti, compresi quelli di Windows Update per tenere aggiornato il sistema operativo.

L'utilizzo di una piattaforma di gestione delle password dotata di adeguate funzionalità di sicurezza per la rete garantisce che tutte le credenziali di accesso aziendali siano conservate al sicuro.

Una caratteristica anti-MITM importante è la crittografia end-to-end che i maggiori software di sicurezza informatica che proteggono milioni di utenti, fra privati e aziende, hanno integrato con la condivisione da cassetta a cassetta utilizzando la PKI (acronimo per Public Key Infrastructure).

Ciò significa che i criminali informatici non possono intercettare le password o altre voci condivise in transito.

L'infrastruttura a chiave pubblica è un insieme di processi e mezzi tecnologici che consentono a terze parti fidate di verificare, o farsi garanti dell'identità di un utente, oltre

CamminoDiritto.it
ISSN 2421-7123

che di associare una chiave pubblica a un utente, normalmente per mezzo di un software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche, tipicamente, assumono la forma di certificati digitali.

Tecnicamente, l'infrastruttura è composta da software client, software server[52] (ad esempio un'autorità di certificazione), hardware (come smart card[53]) e procedure operative. Un utente potrebbe, quindi, firmare i propri messaggi con la sua chiave privata, ed un altro utente controllare questa firma usando la chiave pubblica contenuta nel certificato del mittente, fornito dall'autorità di certificazione facente parte della PKI. Questo meccanismo consente a due, o più, parti desiderose di comunicare di verificare la confidenzialità, l'integrità dei messaggi e l'autenticazione degli utenti senza il bisogno di un precedente scambio di informazioni segrete.

7. Conclusioni

Al netto delle riflessioni compiute circa l'urgenza di sperimentare nuove e alternative forme di proposte contrattuali - un'urgenza, a ben vedere, imposta dall'era mutevole della digitalizzazione dei mercati - non si può non considerare la centralità dei temi che riguardano la protezione della persona dalle insidie tecnologiche pervasive.

Emergono, in tale contesto, i tratti distintivi dei rapporti asimmetrici tra i consumatori e le piattaforme digitali, nonché quelli dei titolari del trattamento dei dati personali che richiedono una protezione normativa convergente tra i settori regolatori contigui della tutela dei consumatori e della tutela dei dati personali.

Pertanto, lo strumentario rimediale protettivo della persona consumatore – contraente debole deve essere, oltre che individuale, anche metaindividuale nel senso di poter rafforzare ulteriormente la protezione nella dimensione collettiva propria delle azioni di classe e, in ultima istanza, anche di deterrente sanzionatorio a tutela della trasparenza e correttezza dei mercati digitali.

Tale convergenza risulta, infatti, in linea con le più recenti evoluzioni normative europee nel solco di un apparato nato con il GDPR e poi evolutosi con la recente direttiva UE 2161/2019[54]. Tutto ciò dimostra come, pur mantenendo fissa la stella polare del Codice civile, anche in Europa il quadro regolatorio si avvia ad un consolidamento delle molteplici fonti e ad un'uniformità di orientamenti che vorranno essere la base per un nuovo mercato unico improntato alle transazioni telematiche di nuova generazione.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Il termine, che deriva dall'inglese e letteralmente significa "confinamento", dall'inizio della pandemia da Covid-19 è stato utilizzato per definire le varie politiche introdotte per contenere i contagi da coronavirus.

[2] Espressione in uso per indicare i principali attori digitali globali, protagonisti non solo delle moderne transazioni telematiche, ma anche della rivalità internazionale che si svolge sulla quinta dimensione.

[3] Da intendersi: il Diritto della tecnologia d'avanguardia, cioè a dire la tecnologia più avanzata disponibile.

[4] Termine breve tratto dalla lingua inglese, concernente l'uso della posta elettronica, con cui si indica il sistema di corrispondenza che consente lo scambio di messaggi tra utenti connessi a una rete di computer, ma situati su computer diversi.

[5] Traducibile in italiano come "rete di ampiezza mondiale", abbreviato Web, sigla WWW o W3, è uno dei principali servizi di Internet, che permette di navigare e usufruire di un insieme molto vasto di contenuti amatoriali e professionali (multimediali e non) collegati tra loro attraverso collegamenti (link), e di ulteriori servizi accessibili agli utenti di Internet;

[6]Nome inglese che tradotto letteralmente significa "disco compatto", abbreviato nella sigla CD), è un tipo standardizzato di disco ottico utilizzato in vari ambiti per la memorizzazione di informazioni in formato digitale.

[7] Una chiave USB (anche in lingua inglese USB flash drive, o pen drive) è una memoria di massa portatile che si collega al computer mediante la porta USB.

[8] [1] M.ORLANDI, Commento all'art.5, 749 s.; R. SIMONE, Testo scritto, cit., 20.

[9] In alternativa, qualche garanzia in tal senso potrebbe derivare dall'impiego di supporti non riscrivibili, come i cd-rom o i dvd – rom. Questo accorgimento è certamente idoneo a garantire che il documento non possa essere modificato dopo la sua creazione, ma non assicura che esso non sia il risultato della manipolazione di altri documenti. Crf. F. RICCI, Scritture private e firme elettroniche, 109, Milano, 2003.

[10] Bit (dall'inglese "binary digit"), in informatica è una cifra binaria, ovvero uno dei due simboli del sistema numerico binario, classicamente chiamati zero (0) e uno (1); si può parlare di numero di 8, 16, 32... bit, come nella comune base dieci si parla di un numero di 8, 16, 32... cifre.

[11] Il software, traducibile come componente logico, programma informatico o supporto logico, in informatica ed elettronica è l'insieme delle componenti immateriali (strato logico/intangibile) di un sistema elettronico di elaborazione.

[12] L'hardware, traducibile in italiano come componente fisico, è la parte materiale di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento.

[13] Attualmente un algoritmo universalmente diffuso per la creazione di coppie di chiavi per la cifratura e la decifrazione dei documenti informatici è l'algoritmo RSA (dal nome dei suoi autori Rivest, Shamir e Adleman). Esso non è sicuro in termini matematicamente dimostrabili. Esiste, perciò, la possibilità teorica che si possa venirne a capo con future scoperte matematiche. Allo stato, tuttavia, l'algoritmo viene ritenuto del tutto affidabile, dal momento che gli studiosi sono concordi nel ritenere che l'eventualità di minarne la base sia enormemente improbabile.

[14] Art. 29 bis, secondo comma, lett.a, t.u.d.a.

[15] Cassazione penale, sezione V, sentenza 14 dicembre 2007, n. 46674

[16] La crittoanalisi (dal greco kryptós, "nascosto", e analýein, "scomporre"), o crittanalisi, è la scienza che studia i metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione. La crittoanalisi è la "controparte" della crittografia, vale a dire lo studio delle tecniche per occultare un messaggio, ed assieme formano la crittologia, la scienza delle scritture nascoste.

CamminoDiritto.it
ISSN 2421-7123

[17] Si ricorre alla cifratura di un'impronta, cioè di una grandezza rappresentata da un valore inferiore a quello che esprime il contenuto del documento, ma è tuttavia funzione di quello, principalmente per rendere più veloci operazioni di calcolo necessarie per la generazione della firma.

[18] Per una spiegazione tecnica del sistema di cifratura a chiavi asimmetriche, si rinvia a P. RIDOLFI, Firma digitale e sicurezza informatica, Milano, 1998.

[19] In crittografia la sigla RSA indica un algoritmo di crittografia asimmetrica, inventato nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman utilizzabile per cifrare o firmare informazioni. Il sistema di crittografia si basa sull'esistenza di due chiavi distinte, che vengono usate per cifrare e decifrare. Se la prima chiave viene usata per la cifratura, la seconda deve necessariamente essere utilizzata per la decifratura e viceversa. La questione fondamentale è che, nonostante le due chiavi siano fra loro dipendenti, non è possibile risalire dall'una all'altra, in modo che se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia.

[20] L'algoritmo DSA (Digital Signature Algorithm) è un algoritmo di firma digitale pubblicato dal NIST nel documento FIPS PUB 186 [1], basato sul problema del logaritmo discreto, analogamente all'algoritmo ElGamal. Una firma digitale DSA viene calcolata attraverso una serie di parametri, tra cui: una chiave privata x e un numero segreto univoco per ogni messaggio. La firma viene verificata attraverso gli stessi parametri, una chiave pubblica associata alla chiave privata utilizzata per creare la firma.

[21] P. RIDOLFI, op.cit.

[22] Ove si ipotizzi l'intervallo compreso fra due valori, ad esempio dieci, elevati in potenza rispettivamente a dieci e a quindici, vi è una quantità enorme di numeri primi, dell'ordine di grandezza di molti miliardi, e chi vuole forzare il sistema deve tentare di combinare tra loro due di questi numeri, nella speranza che l'abbinamento funzioni. La probabilità che il tentativo di crittoanalisi possa riuscire in tempi utili risulta davvero bassa, tanto più che il sistema di generazione delle chiavi deve assicurare "l'equiprobabilità di generazione di tutte le coppie possibili" (art. 5, secondo comma, lett. b, r. tecniche). A ciò si aggiunga che questo esempio si riferisce ad una chiave di soli 128 bit, mentre attualmente "la lunghezza minima delle chiavi è stabilita in 1024 bit" (art. 4, sesto comma, r. tecniche). La robustezza della coppia di chiavi, infatti, è direttamente proporzionale ai bit che la compongono. (M. MICCOLI, Commento all'art. 16, cit., 812).

[23] FINOCCHIARO G., Documento informatico. Il riferimento è al fatto che "la sicurezza del sistema di cifratura non è dimostrabile matematicamente, bensì è di tipo computazionale, ossia è basata sulla considerazione della quantità di lavoro necessario per forzare il sistema, utilizzando l'attuale capacità di calcolo degli elaboratori elettronici".

[24] Metodo forza bruta (anche detto "ricerca esaustiva"), nella sicurezza informatica, indica un algoritmo di risoluzione di un dato problema che consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta. Il suo principale fattore positivo è che esso consente teoricamente di trovare sempre la soluzione corretta ma, per contro, questa è sempre la soluzione più lenta o dispendiosa: viene utilizzato come ultima risorsa sia in crittanalisi, sia in altre parti della matematica, ma solamente in quei casi in cui esso sia l'unico procedimento conosciuto o nei casi in cui altri algoritmi più performanti, tipo l'attacco a dizionario, abbiano fallito.

[25] Con cracking si intende l'accesso ad un sistema informatico non autorizzato utilizzando diverse tecniche informatiche (phishing, exploiting, social engineering, virus come i ransomware etc.).

[26] In crittografia il Data Encryption Standard (DES, letteralmente "Norma per la crittografia dei dati") è un algoritmo di cifratura scelto come standard dal Federal Information Processing Standard (FIPS) per il governo degli Stati Uniti d'America nel 1976 e in seguito diventato di utilizzo internazionale. Si basa su un algoritmo a chiave simmetrica con chiave a 64 bit (ma solo 56 utili poiché 8 sono di controllo).

[27] Attacco man in the middle (spesso abbreviato in MITM, MIM, MIM attack o MITMA, in italiano "uomo nel mezzo") è una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

[28] In crittografia una infrastruttura a chiave pubblica, in inglese public key infrastructure (PKI), è un insieme di

CamminoDiritto.it
ISSN 2421-7123

processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.

[29] Con open source (in italiano sorgente aperto), in informatica, si indica un tipo di software libero da vincoli di copyright o altra natura, nonchè il suo modello di sviluppo o distribuzione.

[30] Nella teoria dei sistemi, un modello black box è un sistema che, similmente ad una scatola nera, è descrivibile essenzialmente nel suo comportamento esterno ovvero solo per come reagisce in uscita (output) a una determinata sollecitazione in ingresso (input), ma il cui funzionamento interno è non visibile o ignoto.

[31] Il Certificato COVID digitale dell'UE (in inglese: EU Digital COVID Certificate, EUDCC) comunemente noto anche come Green Pass, è un certificato interoperabile all'interno dell'Unione europea, contenente le informazioni che attestano che il titolare è stato vaccinato contro la COVID-19, o ha da poco effettuato un test diagnostico per SARS-CoV-2 con risultato negativo, oppure è guarito dalla COVID-19. Il certificato può essere rilasciato sia in formato digitale, sia in formato cartaceo, gratuitamente, in una delle lingue ufficiali dello Stato membro e in lingua inglese. Un codice QR consente di verificare l'autenticità del certificato e la sua validità.

[32] L'RNA messaggero (noto con l'abbreviazione di mRNA o con il termine più generico di trascritto) è un tipo di RNA che codifica e porta informazioni durante la trascrizione dal DNA ai siti della sintesi proteica, per essere sottoposto alla traduzione.

[33] La certificazione verde è necessaria per accedere a: servizi di ristorazione svolti da qualsiasi esercizio per il consumo al tavolo, al chiuso; spettacoli aperti al pubblico, eventi e competizioni sportivi; musei, altri istituti e luoghi della cultura e mostre; piscine, centri natatori, palestre, sport di squadra, centri benessere, anche all'interno di strutture ricettive, limitatamente alle attività al chiuso; sagre e fiere, convegni e congressi; centri termali, parchi tematici e di divertimento; centri culturali, centri sociali e ricreativi, limitatamente alle attività al chiuso e con esclusione dei centri educativi per l'infanzia, compresi i centri estivi, e le relative attività di ristorazione; attività di sale gioco, sale scommesse, sale bingo e casinò; concorsi pubblici.

[34] La maschera facciale filtrante di seconda classe (FFP2) , è un modello di maschera protettiva autofiltrante di tipo usa e getta utilizzata per filtrare il 94% delle particelle aerodisperse, secondo le norme europee EN 143 ed EN 149. La maschera FFP2 è utilizzata nell'industria nonché (senza valvola/valvola per la protezione in entrambe le direzioni) in campo sanitario e medico, in particolare nelle epidemie per evitare malattie trasmissibili e nosocomiali.

[35] In particolare: aeromobili adibiti a servizi commerciali di trasporto di persone; navi e traghetti adibiti a servizi di trasporto interregionale, ad esclusione di quelli impiegati per i collegamenti marittimi nello Stretto di Messina; treni impiegati nei servizi di trasporto ferroviario passeggeri di tipo Inter City, Inter City Notte e Alta Velocità; autobus adibiti a servizi di trasporto di persone, ad offerta indifferenziata, effettuati su strada in modo continuativo o periodico su un percorso che collega più di due regioni ed aventi itinerari, orari, frequenze e prezzi prestabiliti; autobus adibiti a servizi di noleggio con conducente, ad esclusione di quelli impiegati nei servizi aggiuntivi di trasporto pubblico locale e regionale.

[36] Un codice QR (in lingua inglese QR code) è un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all'interno di uno schema bianco di forma quadrata, impiegato in genere per memorizzare informazioni destinate a essere lette tramite un apposito lettore ottico o anche smartphone.

[37] La Commissione europea ha creato una piattaforma tecnica comune per garantire che i certificati emessi da uno Stato possano essere verificati nei 27 Paesi UE più Svizzera, Islanda, Norvegia e Lichtenstein.

[38] La diffusione del SARS-CoV-2 ha generato un'ondata di disinformazione, sia sulla sua origine, sulla sua effettiva grandezza sia sul trattamento del virus. La circolazione di notizie false è stata favorita soprattutto dai social media, dai mass media, e dalle app di messaggistica. Il fenomeno ha avuto un'espansione molto veloce, tant'è che in alcuni Paesi (come Italia e Regno Unito) i vari enti sanitari si sono direttamente attivati avviando campagne informative e pubblicato vademecum per contrastare le fake news maggiormente diffuse. Nel 2022 è stato stimato che le "bufale" sul SARS-CoV-2 generino un giro di affari di circa 1,1 miliardi di dollari annui, causando tuttavia danni agli individui e ai sistemi sanitari nazionali per cifre molto più elevate. Cfr. Hannah Murphy, Mark Di Stefano & Katrina Manson, Huge text message campaigns spread coronavirus fake news, Financial Times, 20 marzo 2020.

[39] Un rogue access point è un access point wireless che è stato installato in una rete sicura da un impiegato

CamminoDiritto.it
ISSN 2421-7123

dell'organizzazione in buona fede o da un aggressore esterno senza un'autorizzazione esplicita da parte dell'amministratore di rete. Cfr. "Rogue-WiFi-Access-point". savegas.com URL.

[40] IP spoofing è la denominazione con la quale si indica, in una rete di computer, una tecnica di attacco informatico che utilizza un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente.

[41] Il DNS spoofing è un attacco informatico, facente parte di una categoria più vasta denominata man in the middle. Il DNS spoofing descrive vari scenari in cui si verifica una manipolazione della risoluzione dei nomi DNS. Nello specifico viene falsificato l'indirizzo IP di un dominio: il terminale stabilisce quindi una connessione all'indirizzo IP falsificato e il traffico di dati viene deviato verso un server fasullo.

[42] In un attacco di spoofing del sito web, il criminale prova a dare un aspetto affidabile a un sito web ingannevole, utilizzando font, colori, logo e altri elementi del layout che appaiono autentici. In genere, questo tipo di attacchi consiste nel creare una replica più o meno precisa di un sito reale, ad esempio quello di una banca online, con l'intenzione di convincere gli utenti a inserire le credenziali di accesso per entrare. Più una copia è fatta bene e più elementi ha in comune con il sito originale, compreso l'URL, che è il primo elemento visualizzato da una persona quando si connette a un sito. A volte cambia solo il tipo di dominio (.net invece di .com) o una lettera nel nome del sito.

[43] Con sniffing (dall'inglese, odorare), in informatica e nelle telecomunicazioni, si definisce l'attività di intercettazione passiva dei dati che transitano in una rete telematica: può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti contro la sicurezza informatica (intercettazione fraudolenta di password o altre informazioni sensibili).

[44] Le tecnologie dell'informazione e della comunicazione (in acronimo TIC o ICT, dall'inglese information and communications technology) sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).

[45] In telecomunicazioni e informatica l'HyperText Transfer Protocol over Secure Socket Layer (HTTPS), (anche noto come HTTP over TLS, HTTP over SSL e HTTP Secure) è un protocollo per la comunicazione sicura attraverso una rete di computer utilizzato su Internet. Consiste nella comunicazione tramite il protocollo HTTP (Hypertext Transfer Protocol) all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (TLS) o dal suo predecessore, Secure Sockets Layer (SSL) fornendo come requisiti chiave: un'autenticazione del sito web visitato; protezione della privacy (riservatezza o confidenzialità); integrità dei dati scambiati tra le parti comunicanti.

[46] La crittografia end-to-end (E2EE) (letteralmente "da un estremo all'altro") è un sistema di comunicazione cifrata nel quale solo le persone che stanno comunicando possono leggere i messaggi. Essa evita che terze parti, compresi gli Internet Service Provider e i gestori delle reti di telecomunicazione, possano leggere o alterare i messaggi scambiati tra due persone. Agli intermediari non è consentito l'accesso alle chiavi di cifratura, evitando così tentativi di sorveglianza o alterazione dei messaggi scambiati.

[47] Nell'informatica, nell'ambito delle reti di computer, un firewall (termine inglese dal significato originario di parete refrattaria, muro tagliafuoco, muro ignifugo; in italiano anche parafuoco o parafiamma) è un componente hardware e/o software di difesa perimetrale di una rete, originariamente passivo, che può anche svolgere funzioni di collegamento tra due o più segmenti di rete, fornendo dunque una protezione in termini di sicurezza informatica della rete stessa.

[48] Il consulente di direzione (consulente di management) è un professionista competente nella consulenza per la conduzione di un'organizzazione nella sua gestione strutturale e per il miglioramento dei processi.

[49] Un hotspot è un luogo fisico in cui le persone possono accedere a Internet, in genere tramite Wi-Fi, sfruttando una rete locale senza fili (WLAN) con un router collegato a un provider Internet. Ci si riferisce a questi luoghi con i termini "hotspot Wi-Fi" o "connessioni Wi-Fi".

[50] Una rete virtuale privata (tradotto dall'inglese in lingua italiana letteralmente: Virtual Private Network, acronimo: VPN), nelle telecomunicazioni, è una rete di telecomunicazioni privata, instaurata come connessione tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la suite di protocolli Internet.

[51] Malware è una forma contratta, tratta dalla lingua inglese, che viene utilizzata per indicare un "malicious

CamminoDiritto.it
ISSN 2421-7123

software", ovvero un software male intenzionato o malevolo. Nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer. Termine coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer; in italiano viene anche comunemente chiamato codice maligno.

[52] In informatica il termine sistema client-server (letteralmente cliente-serviente) indica un'architettura di rete nella quale genericamente un computer client o terminale si connette ad un server per la fruizione di un certo servizio, quale ad esempio la condivisione di una certa risorsa hardware/software con altri client, appoggiandosi alla sottostante architettura protocollare.

[53] Una carta intelligente (in inglese smart card) è un dispositivo hardware che possiede potenzialità di elaborazione e memorizzazione dati in grado di garantire elevati standard di sicurezza. Più in generale, un insieme di tecnologie, comprendenti circuiti integrati, microprocessori, memorie RAM, ROM, EEPROM, antenne, ecc., integrate nello stesso circuito elettrico per formare un circuito integrato che ne costituisce il nucleo principale.

[54] DIRETTIVA (UE) 2019/2161 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=8132