Gruppo VII

Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica

Sottogruppo: Reati contro la riservatezza e la sicurezza informatiche, nonché l'identità digitale

Lorenzo Picotti, Roberto Flor, Ivan Salvadori (Università di Verona)

Sommario: 1. Premessa sui beni giuridici protetti. – 2. Proposta di ricollocazione sistematica. – 3. I reati contro la riservatezza informatica. – 3.1. Accesso non autorizzato ad un sistema informatico – 3.1.1. Ragioni della riforma. – 3.1.2. Accesso non autorizzato ad un sistema informatico e circostanze aggravanti. – 3.2. Diffusione abusiva di codici di accesso ad un sistema informatico. – 3.3. La tutela delle "comunicazioni informatiche". – 3.3.1. Proposta di introduzione del nuovo delitto di violazione della riservatezza delle comunicazioni informatiche. - 4. I reati contro la sicurezza informatica. - 4.1. Diffusione abusiva di dispositivi diretti a danneggiare un sistema informatico. – 4.2. La nozione di "interferenze non autorizzate" in ambito informatico. - 5. La tutela penale dell'identità digitale. – 5.1. Le principali criticità. – 5.2. Proposte di riforma. – 6. Proposta di articolato

1. Premessa sui beni giuridici protetti

Sviluppando le riflessioni critiche sintetizzate nella relazione presentata al Convegno di Torino del 9 e 10 novembre 2018 sulle vigenti fattispecie penali in materia di violazioni della riservatezza e sicurezza informatiche, di cui si erano evidenziati i limiti applicativi e sistematici, e talora l'obsolescenza, nel successivo Convegno di Napoli del 30 e 31 maggio 2019 sono state presentate le proposte di riformulazione o nuova previsione di fattispecie penali in tale ambito, a partire dalla necessità di un migliore inquadramento sistematico e, quindi, di una più convincente collocazione topografica, che sia non solo più corretta teoricamente, ma anche più immediatamente comprensibile per i destinatari (sia operatori giuridici, che cittadini).

Si è sottolineata anche l'esigenza di una maggiore coerenza con le previsioni e raccomandazioni contenute nelle fonti sovranazionali, che considerano, quale nucleo fondamentale comune degli interessi giuridici meritevoli di tutela penale in questo campo, la c.d. triade *CIA* (*Confidentiality, Integrity, Availability*: letteralmente "confidenzialità, integrità e disponibilità" dei dati e dei sistemi informatici), cui è espressamente dedicato il Titolo I (comprendente gli artt. da 2 a 6) della Sezione relativa al diritto penale sostanziale del Capitolo II della Convenzione *Cybercrime* del Consiglio d'Europa del 2001. Ed anche la Direttiva 2013/40/UE del 12 agosto 2018, relativa agli attacchi ai sistemi di informazione, prevede agli artt. da 3 a 7 sostanzialmente gli stessi precetti, seppur con elementi costitutivi in parte diversamente formulati; mentre la più recente Direttiva 2016/1148/UE del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti

e dei sistemi informativi dell'Unione, cui ha fatto seguito un importante Regolamento d'esecuzione nel 2018, all'art. 4, n. 2, definisce la nozione di "*sicurezza della rete e dei sistemi informativi*" quale "*capacità di resistere*" ad azioni che compromettano "*l'autenticità, l'integrità o la riservatezza dei dati*". Tale sempre più forte esigenza di "sicurezza cibernetica" (*cybersecurity*), presente anche nel Regolamento UE 2016/679 del 27 aprile 2016 sulla protezione dei dati personali (GDPR), che peraltro non obbliga a prevedere sanzioni penali, ma stabilisce direttamente solo forti sanzioni amministrative per sanzionare le violazioni di precetti che devono garantirla, quale necessario *pendant* della *privacy*, si è da ultimo imposta come decisamente dominante, di fronte ai sempre più forti rischi di attacchi informatici ed alle gravissime conseguenze che possono avere, nell'intero settore dei sistemi di informazione e delle reti di comunicazione, a prescindere dalla tecnologia utilizzata, per la loro sempre più forte estensione, integrazione e potenza di connessione, come palesemente emerge nel più recente decreto legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di "perimetro di sicurezza nazionale cibernetica".

Per queste chiare tendenze di sviluppo, riscontrabili a livello globale e correlate ad evidenti ragioni strutturali d'impetuosa evoluzione ed espansione dello spazio cibernetico in cui siamo sempre più immersi (il c.d. *Cyberspace*), occorre, da un lato, ribadire l'importanza fondamentale e crescente delle specifiche esigenze di tutela penale della "riservatezza" e della "sicurezza" *informatiche*, dall'altro riconoscere la loro strettissima connessione, che porta addirittura a ricomprenderle nell'ampia ed articolata nozione di *cybersecurity*.

2. Proposta di ricollocazione sistematica

Per le esposte ragioni strutturali, nonostante la contiguità con i beni giuridici della riservatezza della corrispondenza e delle comunicazioni "personali", dopo ampio dibattito all'interno del nostro *team* e tenendo conto di quanto emerso nell'incontro del Gruppo svoltosi il 2 dicembre 2019 a Torino, è prevalsa la scelta di mantenere la proposta di una nuova ed autonoma "Sezione VI" da aggiungere all'interno del capo III («*Delitti contro la libertà individuale*») del Titolo XII («*Delitti contro la persona*») del Libro II del codice penale, denominata: "*Dei delitti contro la riservatezza e la sicurezza informatiche*".

Infatti, gli aspetti *specifici* che caratterizzano tali beni, qualificati dall'intreccio strettissimo con le concomitanti esigenze di tutela delle reti e dei sistemi informatici, che necessariamente veicolano le odierne forme di espressione, gestione, trattamento della comunicazione e diffusione dei dati ed informazioni nel *Cyberspace*, superando ed assorbendo i profili di interrelazione immediatamente od esclusivamente "fra persone" (basti pensare al ruolo che oggi svolgono i sempre

più sofisticati algoritmi, sistemi di intelligenza artificiale e *machine learning* nella stessa elaborazione, selezione, indirizzamento di informazioni e trasmissioni il cui *input* soltanto può essere originariamente "personale"), porta a ritenere prevalente l'esigenza di autonomia anche sistematica, oltre che strutturale, delle nuove fattispecie, così in grado, fra l'altro, di esercitare un più chiaro ruolo di richiamo ed attenzione sia verso i destinatari, sia verso gli operatori giuridici (pubblici ministeri, giudici, forze di polizia, avvocati), per le predette nuove e peculiari esigenze di protezione penale.

Del resto, riesaminando il contenuto delle condotte e delle tipologie di eventi o risultati ad esse correlati, compresa l'individuazione del loro peculiare momento consumativo, avente rilevanti ricadute anche sulla determinazione del *locus commissi delicti* con relative conseguenze processuali, si rafforza la necessità di un'autonoma tipizzazione normativa dei fatti illeciti che non necessariamente hanno ad oggetto un "contenuto personale" o rispetto ai quali può mancare l'intermediazione di una persona (si pensi, a titolo paradigmatico, alle «*comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi*» di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.), rispetto a quella delle tradizionali fattispecie in materia di segretezza della corrispondenza e delle altre forme di comunicazione, dove, già nella formulazione del fatto tipico, emerge la necessaria mediazione di una persona umana (si pensi, ad es., alle condotte consistenti nel «*prendere cognizione del contenuto di una corrispondenza chiusa*» o nel «*sottrarre o distrarre, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta*» di cui all'art. 616 c.p.).

In tale nuova Sezione VI dovrebbero dunque raggrupparsi le diverse fattispecie – in parte da riformulare, in parte da aggiungere – poste a presidio della "*confidenzialità, integrità e disponibilità*" (*CIA*) dei dati, dei sistemi informatici e delle relative comunicazioni, oltre che della *"autenticità"* dei trattamenti automatizzati, che sostituiscono l'intermediazione diretta dell'uomo quale persona fisica, essendo ormai chiaramente emersa, a partire dalle fonti sovranazionali, l'esigenza di loro *specifica* protezione penale, che si estende logicamente a quella dell'"*identità digitale*", di fronte ai preoccupanti fenomeni di falsificazione ed usurpazione fraudolenta che si manifestano ad es. nei *social network* e nello spazio cibernetico in genere (ad es. con la massiccia creazione di false identità, *fake news*, ecc.).

Si tratta di delitti che offendono beni comunque riferibili alla persona, intesa in un senso molto ampio ed indiretto, essendovi sempre, "dietro" le comunicazioni ed i trattamenti informatici , una persona umana od un ente: per cui si giustifica (almeno allo stato) la collocazione nel Titolo XII, ed in specie nel Capo III dedicato alla "Libertà morale".

Ma si tratta di beni che si distinguono, nella loro configurazione strutturale e nelle relative modalità d'offesa, innanzitutto dalla sfera di tutela del domicilio (Sezione IV), che appare opportuno

lasciare ancorata alla tradizionale nozione fisico-spaziale, abbandonando la forzosa estensione anche a quella "*informatica*", che era stata operata in una fase di primo approccio alla nuova realtà tecnologica dal legislatore del 1993. Proprio le numerose novelle successive, seppur spesso non condivisibili sul piano delle scelte di politica criminale, in materia di furti nel domicilio e di legittima difesa domiciliare, dimostrano il forte e preponderante riferimento a detta (sola) accezione originaria.

D'altro lato, la "*riservatezza e sicurezza informatiche*" vanno distinte sia dall'oggetto di tutela dei reati – ed oggi, dopo l'entrata in vigore del Regolamento europeo 2016/679 (GDPR) e delle norme nazionali, anche penali, di adeguamento di cui al d.lgs. 10 agosto 2018, n. 101, soprattutto degli illeciti amministrativi - in materia di tutela dei dati "personali" (che come si è sottolineato fin dalla relazione presentata al convegno di Torino del 2018 garantiscono il rispetto delle regole e condizioni stabilite dalla specifica ed articolata disciplina extrapenale in materia), sia dalla sfera di tutela dei "*segreti*" propriamente intesi, di cui alla Sezione V del Capo in questione, compresi quelli epistolari e delle comunicazioni interpersonali strettamente intese (telegrafiche e telefoniche, in specie), in quanto vengono in rilievo esigenze di protezione più specifiche, da distinguere - come si è sopra già argomentato - dal nucleo più ristretto di esclusione 'assoluta' dall'accesso al contenuto di informazioni o notizie immediatamente espresse da "persone" in una relazione diretta con altri, rispetto a chiunque ne sia estraneo o non sia autorizzato dal titolare o comunque non ne abbia il consenso.

Concettualmente, nella predetta nuova Sezione VI si potrebbero suddistinguere tre gruppi fondamentali di delitti.

Un primo gruppo dovrebbe riguardare la "*riservatezza informatica*" intesa quale "*confidenzialità*" (non segretezza in senso stretto) e "*disponibilità*" dei dati, dei sistemi e delle stesse reti (in sintesi: di "spazi" informatici, ovunque si trovino, anche nel c.d. *cloud*), di pertinenza non solo di una persona fisica, ma anche di un ente o di una persona giuridica. Vi si devono quindi comprendere: a) il delitto di "*accesso non autorizzato*" ad un sistema informatico (attuale art. 615-*ter* c.p., peraltro da emendare); b) quello prodromico di "*produzione e diffusione*" di codici di accesso (attuale art. 615-*quater* c.p., parimenti da emendare); c) le *"interferenze nelle comunicazioni informatiche*"[1], compresa la corrispondenza elettronica (attuale art. 616, ultimo comma, c.p., da scorporare dall'equiparazione alla corrispondenza tradizionale, anche per quanto riguarda la tipologia delle condotte punibili), nonché altre forme di comunicazioni a distanza, cui già si richiama la disposizione estensiva di cui all'art. 623-*bis* c.p., che ne verrebbe assorbita; d) le "*intercettazioni informatiche e telematiche"* strettamente intese (attuale artt. 617-*quater* c.p., da emendare e

[1] Sulla proposta di introduzione di un nuovo delitto di interferenze non autorizzate nelle comunicazioni informatiche di contenuto riservato v. *infra*, par. 3.3.1.

semplificare), da ricondurre alle ipotesi di "interferenza" nelle menzionate comunicazioni informatiche; e) il delitto prodromico di "*installazione di dispositivi atti ad intercettare, impedire od interrompere comunicazioni informatiche e telematiche*" (attuale art. 617-*quinquies* c.p., parimenti da emendare).

Un secondo gruppo di delitti dovrebbe riguardare la "*sicurezza informatica*" più strettamente intesa, quale integrità ed autenticità dei dati, oltre che dei sistemi e dei trattamenti anche in rete, e comprendere: a) i vari delitti di "*danneggiamento informatico*" (attuali artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p., che sarebbero da ricollocare al di fuori dei delitti contro il patrimonio, in cui oggi si trovano, oltre che da semplificare e riformulare); b) il delitto prodromico di "*produzione e diffusione di dispositivi idonei a danneggiare*" (attuale art. 615-*quinquies* c.p., peraltro da emendare); c) la norma definitoria della c.d. "*violenza informatica*", da ridenominare più opportunamente come "*interferenze non autorizzate in ambito informatico*", emendando la formulazione e collocazione attuale di cui all'art. 392, comma 3, c.p., da comprendere nella nuova Sezione VI, trasponendola dal Titolo II dei delitti contro l'amministrazione della giustizia, in cui era stata attratta dal legislatore del 1993 per l'esigenza contingente di estendere l'ambito applicativo del delitto di esercizio arbitrario del proprie ragioni "*mediante violenza sulle cose*", punito da detto articolo. Questa arbitraria modalità di condotta, che è improprio denominare "violenta" od assimilare alla "violenza sulle cose", dato il pregnante significato fisco-materiale di quest'ultimo tradizionale concetto, che rimanda ad una specifica energia fisica esercitata su di un oggetto materiale, può in effetti caratterizzare anche altri delitti, ad es. contro il patrimonio, come nel caso dell'estorsione (art. 629 c.p.) commessa mediante illecita criptazione di dati e sistemi altrui (ad es. impiegando *ransomware*) ovvero contro l'economia pubblica, come nel caso della turbata libertà dell'industria o del commercio (art. 513 c.p.); e dovrebbe comprendere tutte quelle interferenze e quegli interventi arbitrari e dannosi su dati e *software*, che violino, oltre alla loro "*integrità*" strettamente intesa, anche la loro "*autenticità*" intesa come provenienza o riferibilità genuina all'autore o comunque al soggetto titolare del trattamento e dei dati e legittimato ad operarvi, intaccando la stessa "*funzionalità*" del processo di elaborazione all'utilizzo o destinazione voluti da chi ne ha diritto.

Infine, in chiusura della nuova Sezione VI dovrebbe essere previsto il nuovo delitto di "*violazione dell'identità digitale*", con contestuale abrogazione dell'attuale comma 3 dell'art. 640-*ter* c.p., che è oggi applicabile alla sola frode informatica, quale sua ipotesi aggravata, ma che invece, debitamente riformulato, dovrebbe avere una portata generale, assorbendo anche lo spazio oggi affidato dalla giurisprudenza al più lieve reato di sostituzione di persona, di cui all'art. 494 c.p.

3. I reati contro la riservatezza informatica

3.1. Accesso non autorizzato ad un sistema informatico

Art. 2 CoC	Art. Direttiva 2013/40/UE
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **access to the whole or any part of a computer system without right**. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	Member States shall take the necessary measures to ensure that, when committed intentionally, the **access without right, to the whole or to any part of an information system**, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

Art. 615-*ter* c.p. ***Accesso abusivo ad un sistema informatico o telematico***	**Proposta di riforma art. 615-*ter* c.p.** ***Accesso non autorizzato ad un sistema informatico***[2]
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.	*Chiunque **accede**[3] senza autorizzazione o eccedendone i limiti ad un sistema informatico o ad una sua parte è punito, a querela della persona offesa, con la reclusione fino a tre anni.*

[2] Pare opportuno sopprimere l'aggettivo «telematico», in quanto il concetto di "sistema informatico" è di per sé idoneo a ricomprendere anche i sistemi di elaborazione tra loro interconnessi o connessi alla rete Internet.

[3] La descrizione della condotta tipica in termini di «*accesso*» ad un sistema informatico, in luogo del discutibile termine «*introdursi*», che presuppone l'introduzione in uno spazio "fisico" (come, ad es., un domicilio), pare sicuramente più corretta e conforme al linguaggio informatico ed alle indicazioni di fonte sovranazionale, oltre che alla stessa rubrica dell'art. 615-*ter* c.p.

La dicotomia della condotta tipica (in termini di "introduzione" e "mantenimento") è stata (e continua ad essere) causa di notevoli problemi ed equivoci in giurisprudenza ed in dottrina (v., ad es., le recenti sentenze della Cassazione SS.UU. del 7 febbraio 2012, n. 4694 e, più di recente, dell'8 settembre 2017, n. 41210). Più corretta pare pertanto l'incriminazione del mero *accesso non autorizzato* (o «*abusivo*»), in quanto idonea a ricomprendere le ipotesi di accesso non autorizzato poste in essere dai c.d. *outsider* (che operano in assenza di autorizzazione), oltre che quelle dei c.d. *insider* che accedono, in tutto o in parte, ad un sistema informatico, *eccedendo* i limiti dell'autorizzazione, come già riscontrato nella prassi giurisprudenziale ed, in prospettiva comparata, negli Stati Uniti, tanto a livello federale quanto statale, nonché nella legislazione penale belga. La scelta politico-criminale di incriminare, oltre alla condotta di "intrusione", anche quella omissiva di "permanenza" (*rectius* "mantenimento") in un sistema informatico non trova riscontro a livello sovranazionale e neppure nella maggior parte degli ordinamenti giuridici europei ed extraeuropei, salvo alcune rare eccezioni (Francia, Belgio, Spagna e Turchia).

3.1.1. Ragioni della riforma

Tra le condotte di accesso non autorizzato ad un sistema informatico meritano di essere punite, in linea con le indicazioni di fonte sovranazionale, soltanto quelle che sono proiettate, nella loro direzione offensiva, contro l'interesse di un altro utente (sia esso persona fisica o giuridica od ente) al godimento esclusivo, sicuro ed indisturbato degli "spazi" informatici (c.d. *riservatezza informatica*) e solo indirettamente contro l'interesse giuridico della *sicurezza informatica,* che assume ormai dimensione super-individuale o collettiva, per l'interconnessione pressoché permanente dei diversi sistemi e dispositivi anche mobil*i.* In tal senso è da condividere la scelta politico-criminale di molti legislatori nazionali (ad. es. spagnolo, tedesco ed austriaco) che, in conformità con le prescrizioni e gli obblighi di incriminazione di fonte sovranazionale (art. 2 CoC ed art. 3 della direttiva europea 2013/40/UE), hanno limitato l'ambito del penalmente rilevante alle condotte di "accesso non autorizzato" a sistemi informatici poste in essere *violando* le misure di sicurezza (*«[die] Überwindung der Zugangssicherung*» - § 202a StGB; *«[die] Überwindung einer spezifischen Sicherheitsvorkehrung*» - §118a Ö-StGB; «*vulnerando las medidas de seguridad* » - art. 197-*bis*.1 CP Sp.) destinate a proteggerli.

Mediante tale formulazione, la *relazione conflittuale fra portatori di interessi contrapposti* diventa, in un contesto virtuale, più facilmente percepibile e riconoscibile dal soggetto agente. Nel momento in cui l'utente "*senza autorizzazione*" viola una misura di sicurezza posta a protezione di un sistema informatico altrui, eccede consapevolmente i limiti della libertà di accesso e di navigazione nel *Cyberspace.*

La previsione, quale requisito tipico di fattispecie, della *oggettiva violazione delle misure di sicurezza* poste a protezione del sistema, porterebbe, tuttavia, ad escludere la rilevanza penale delle condotte sempre più frequenti dei dipendenti, dei funzionari pubblici e, più in generale, dei c.d. *insider* che, eccedendo i limiti dell'accesso consentito, accedono a spazi o ambiti non protetti di un sistema informatico (di un *Cloud*, di un *Server*, di una banca dati, ecc.) per consultare, copiare, comunicare o danneggiare dati ed informazioni. La loro condotta non potrebbe essere sanzionata penalmente, dal momento che l'iniziale *accesso* al sistema avviene attraverso l'impiego legittimo delle credenziali di autenticazione, compresa la *password*, fornite dal datore di lavoro o dal titolare del sistema. Di conseguenza, manca l'oggettiva violazione di misure (tecniche) di sicurezza, che invece in caso di *outsider* viene assorbita nel carattere "*non autorizzato*" (od *abusivo*) dell'accesso.

Viste le difficoltà ermeneutiche ed applicative incontrate nella sussunzione di questa tipologia di condotte nell'ipotesi attualmente prevista del "*mantenimento*" nel sistema informatico, contro la volontà espressa o tacita del titolare, in prospettiva *de jure condendo* si potrebbe riformulare

il reato di accesso abusivo, sopprimendo tale ipotesi alternativa e prendendo come modello la fattispecie di «*accesso illecito a sistemi di informazione*» prevista dall'art. 2 CoC. La condivisibile scelta politico-criminale del Consiglio d'Europa è di sanzionare la mera condotta di «*accesso non autorizzato ad un sistema informatico o ad una sua parte*», a prescindere dal requisito della *violazione* di misure di sicurezza, la cui previsione, quale requisito di fattispecie, è lasciata alla discrezionalità dei singoli legislatori nazionali.

L'espressa incriminazione del semplice "*accesso*" non autorizzato (o "*abusivo*"), in luogo dell'attuale "*introdursi*", oltre ad essere più coerente con il riferimento all'ipotesi che avvenga anche soltanto "*ad una parte*" di un sistema informatico, presenterebbe il vantaggio di permettere l'incriminazione degli accessi abusivi realizzati non solo dai c.d. *outsider* (ad es. *hacker* e *cracker*), ma anche dai dipendenti, incaricati od, in generale, *insider* che, possedendo legittimamente le credenziali di autenticazione per "introdursi" in un sistema informatico, si spingono però oltre i limiti dell'autorizzazione ed operano ulteriormente, accedendo "*senza autorizzazione*" anche a parti o "spazi" riservati, che sarebbero loro preclusi dal titolare o dall'ambito del loro competenze.

Il carattere *abusivo* o, meglio, "*non autorizzato*" dell'"intrusione" in un sistema informatico da parte di un *insider* dovrebbe stabilirsi sulla base della violazione di specifici regolamenti interni, norme o disposizioni aziendali anche di natura contrattuale o comunque norme extrapenali, pur non necessariamente specifiche per la regolazione degli accessi, ma inerenti alle finalità ed ai contenuti delle mansioni affidate, sulla cui base si possa anche determinare in modo chiaro a quali spazi della memoria o del sistema od a quali dati ed archivi il dipendente o l'incaricato possa accedere nell'esercizio delle sue mansioni o per le "ragioni" o funzioni per cui l'accesso è consentito. In presenza di tali regole extrapenali, anche di tipo tecnico-informatico, che stabiliscano gli ambiti e gli spazi di accesso autorizzato o le ragioni/funzioni per le quali esso è autorizzato, il giudice potrà determinare in modo oggettivo se la condotta posta in essere dall'*insider* sia da qualificare o meno come autorizzata dal titolare del sistema e, quindi, penalmente rilevante od irrilevante. Attraverso questa interpretazione restrittiva del requisito della "*mancanza di autorizzazione*", da intendersi quale *clausola di illiceità speciale*, che contribuisce alla tipizzazione oggettiva del fatto di reato, si eviterebbero quegli errori emersi nella prassi applicativa, che hanno portato a dar rilievo invece alle finalità personali o soggettive dell'*insider*.

3.1.2. Accesso non autorizzato ad un sistema informatico e circostanza aggravanti

Art. 9 Direttiva 2013/40/UE

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:

*(a)they are committed **within the framework of a criminal organization**, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;*

*(b) **they cause serious damage**; or*

*(c) they **are committed against a critical infrastructure information system**.*

Art. 615-*ter*, comma 2, c.p.	**Proposta di riforma**
La pena è della reclusione da uno a cinque anni:	La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;	1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di **amministratore od operatore di sistema**[4];
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;	2) se il colpevole per commettere il fatto usa violenza sulle cose o pone in essere interferenze non autorizzate in ambito informatico[5]
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la	

[4] Appare opportuno prevedere anche la figura dell'"*amministratore di sistema*" («*system administator*») che indica quei soggetti qualificati anche sul piano tecnico-informatico, che avendo il controllo delle fasi del processo di elaborazione e trattamento di dati informatici, possono disporre l'accesso con maggiore facilità ai sistemi informatici sui quali hanno competenza.

[5] L'aggravante, nella formulazione oggi vigente, nella parte in cui contempla l'ipotesi del soggetto che accede abusivamente ad un sistema informatico «*con violenza alle persone*» ovvero di intrusione da parte di un soggetto «*palesemente armato*», possiede, come dimostra la sua scarsa (se non inesistente) applicazione giurisprudenziale, un ruolo del tutto marginale. Tale circostanza aggravante aveva un senso nell'epoca in cui, non essendo ancora diffusa l'interconnessione tra i *computer*, gli attacchi informatici presupponevano un contatto fisico con l'elaboratore c.d *stand alone*. Con la progressiva e capillare diffusione delle reti telematiche, ed in specie di Internet, non è più necessario ed è anzi eccezionale che per introdursi abusivamente in un *computer* vi sia un contatto fisico con l'elaboratore attaccato o con le persone eventualmente addette alla sua sorveglianza. I criminali informatici (in specie *hacker* e *cracker*) invero sfruttano la rete per accedervi da remoto.
La modalità della "*violenza sulle cose*" deve estendersi anche alle specifiche "*interferenze non autorizzate in ambito informatico*" quali definite oggi dal comma 3 dell'art. 392 c.p. e impropriamente ricondotte alla nozione di "violenza" c.d. informatica, di cui sopra si fatto cenno (par. 2) e di cui meglio si dirà (infra par. 4.2).

distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. co. 3) Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.	**3) abrogata**[6] **co. 3)** Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici **di pubblica utilità**[7] **o di una infrastruttura critica**, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. **co. 4)** ***se il fatto è commesso nell'ambito di una associazione per delinquere***[8] Nel caso previsto dal primo comma[9] il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

3.2. Diffusione abusiva di codici di accesso ad un sistema informatico

Art. 6 CoC	Art. 7 Direttiva 2013/40/UE
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: I a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making

[6] In luogo della vigente previsione, che integra una controversa ipotesi di reato aggravato dall'evento, pare più corretto ricorrere, nel caso in cui ad un accesso abusivo ad un sistema informatico consegua il danneggiamento di dati informatici o dello stesso sistema informatico, alla più generale disciplina normativa in materia di concorso di reati, con la conseguenza che i delitti di danneggiamento informatico restano punibili solo a titolo di dolo.

[7] Tale sintetica, e più apprezzabile locuzione, impiegata dal legislatore anche in altre disposizioni, avrebbe il merito di ovviare all'altrimenti poco esaustiva elencazione dei sistemi informatici "pubblici" meritevoli di una tutela penale rafforzata, prevista dall'attuale ipotesi delittuosa dell'art. 615-*ter*, co. 3, c.p.

[8] In linea con quanto previsto dalla citata direttiva 2013/40/UE.

[9] V. *supra* par. 3.1. per la nuova riformulazione dell'art. 615-*ter*, co. 1, c.p.

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor: (a)a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6; (b)a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Art. 615-*quater* c.p. ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici***	**Proposta di riforma** ***Produzione e diffusione non autorizzata di codici di accesso ad un sistema informatico***
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è	**Fuori dai casi previsti dall'articolo precedente**[10], chiunque, al fine di procurare a sé o ad altri un **ingiusto** profitto o di arrecare ad altri un danno, abusivamente **produce**, procura **per sé o per altri**, riproduce, diffonde, comunica o consegna codici, ***password***[11], **dati informatici** o altri mezzi idonei all'**accesso non autorizzato ad un sistema**

[10] La previsione di questa clausola di riserva ha lo scopo di evitare che il menzionato delitto preparatorio possa concorrere con quello più grave di accesso abusivo ad un sistema informatico di cui all'art. 615-*ter* c.p.

[11] L'impiego del concetto di "*password*", in luogo del meno appropriato «*parole chiave*», oltre ad essere più adeguata sul piano tecnico-informatico, è in linea con le prescrizioni di fonte sovranazionale.

punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.	**informatico**, è punito on la reclusione sino **a due anni** e con la multa sino a euro 10.329[12].
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.	La pena è della reclusione da uno a **tre** anni e della multa da euro 5.164 a euro **15.492** ***se ricorre taluna delle circostanze di cui al secondo, terzo e quarto comma dell'art. 615-ter c.p.***[13] [NB:Il delitto è perseguibile d'ufficio].

3.3. La tutela delle "comunicazioni informatiche e telematiche"

Lo sviluppo impetuoso delle tipologie di comunicazione informatica, rispetto al tempo in cui è stata emanata la prima legge contro la criminalità informatica del 23 dicembre 1993, n. 547, richiede una profonda revisione che vada oltre la mera estensione, allora introdotta, delle disposizioni concernenti la corrispondenza epistolare tradizionale (art. 616 e seguenti c.p.) a quella "*informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*", peraltro non specificamente definita e cui sono però così riferite le identiche tipologie di condotte, già previste con riferimento a detta corrispondenza tradizionale.

Non solo sono mutati i mezzi di comunicazione, i cui oggetti sono del tutto smaterializzati, ma grazie all'interconnettività pressoché permanente in rete, all'aumentata capacità dei dispositivi mobili (*tablet* e *smartphone* soprattutto), all'intervento sempre più massiccio ed incisivo di sofisticati algoritmi e sistemi di intelligenza artificiale nella stessa elaborazione, selezione, indirizzamento di informazioni e trasmissioni solo originariamente "personali", questi sono in grado di trasmettere e ricevere in ogni momento e luogo, anche a grandi distanze, successioni o ripetizioni temporali, *file* di testo, voci, suoni, immagini, anche in movimento, video di grandi dimensioni, loro elaborazioni o riproduzioni. Inoltre si sono moltiplicati e sviluppati i "servizi" che offre la rete, con conseguenti nuove possibilità e modalità di comunicazione e rielaborazione, che vanno ben oltre le comuni *e-mail*, essendosi espansa la messaggistica di ogni genere, ed in specie la possibilità di condivisione,

[12] Pare opportuno sopprimere la condotta, ulteriormente prodromica, del «fornire indicazioni o istruzioni idonee ad accedere ad un sistema informatico o telematico», dal momento che, in violazione del principio di offensività, porta ad una eccessiva anticipazione della tutela penale rispetto al bene giuridico della riservatezza informatica e, indirettamente, della sicurezza informatica, punendo il "*pericolo di un pericolo*", vale a dire il *pericolo* di procurarsi o di produrre un codice di accesso, la cui disponibilità fa sorgere il *pericolo* di un accesso abusivo ad un sistema informatico. Le pene vengono peraltro allineate a quelle previste dall'attuale art. 615-*quinquies* (su cui cfr. *infra* par. 4.1), non essendo il pericolo di offesa al bene giuridico della riservatezza informatica da considerare meno grave del pericolo di offesa a quello della sicurezza informatica, del resto strettamente collegato all'altro.

[13] Trattandosi di una norma incriminatrice che punisce comportamenti prodromici e preparatori all'accesso abusivo ad un sistema informatico è senz'altro più corretto e coerente richiamare le circostanze aggravanti di cui all'art. 615-*ter* c.p.

circolazione, riproduzione, ecc., in gruppi, chat, ambiti estesi o ristretti di utenti, ecc., di qualsiasi genere di dati, come si può emblematicamente riscontrare nell'uso dei più diffusi *social network* (quali *Facebook*, *Instagram*, *Twitter*, *WhatsApp*, ecc.).

Corrispondentemente si sono modificate le stesse tipologie di condotte, che possono violarne la riservatezza, la disponibilità, l'autenticità e l'integrità, con conseguente necessità di introdurre un'autonoma tipizzazione dei fatti che offendano tali beni giuridici, che come detto incorporano specificamente la riservatezza e la sicurezza informatiche.

Nel contempo vi è anche l'esigenza che le fattispecie di diritto penale sostanziale a tutela delle "*comunicazioni informatiche*" tengano conto della disciplina processuale relativa alla ricerca ed acquisizione delle c.d. prove elettroniche, che proprio per garantire con diversa intensità i diritti e gli interessi diversi che possono venire compressi, valorizza alcune tradizionali distinzioni imperniate sulla differenza fra la corrispondenza, le conversazioni, le comunicazioni o le trasmissioni, anche informatiche o telematiche, ovvero genericamente i "documenti".

In specie, sembra necessario offrire maggior protezione al "flusso" *dinamico* di comunicazioni "*in corso*", le violazioni o compressioni della cui riservatezza vanno inquadrate nella disciplina sostanziale (attuali artt. 617 segg., in specie 617-*quater* segg. c.p.) oltre che processuale delle "*intercettazioni informatiche*"; laddove rispetto a contenuti in qualche modo già "cristallizzati" in *file* e dati memorizzati, che presentano una "staticità" di informazioni e notizie già comunicate, analoga a quella della "corrispondenza" tradizionalmente intesa, può essere modulato un livello di tutela (sostanziale e processuale) differenziato.

Alla stregua del codice di procedura penale, all'acquisizione della "*corrispondenza*", compresa quella informatica, si procede con lo strumento della perquisizione (art. 247, in specie comma 1-*bis* c.p.p.) e del sequestro (artt. 253 e 254, nonché 254-*bis* c.p.p.), che è applicabile anche all'ampia categoria dei "documenti", compresi quelli informatici (artt. 234 e 234-*bis* c.p.p.). Viceversa, nel caso delle "*intercettazioni*" occorre procedere, per il carattere più invasivo e dinamico che possono avere, interferendo con il "flusso" comunicativo in atto, tramite appositi strumenti tecnici (ad es. mediante *Trojan* o programmi *spyware*), previa autorizzazione e delimitazione della durata ed estensione da parte del Giudice, sulla base di requisiti più stringenti, che presuppongono già la presenza di qualificati elementi di sospetto, assicurando garanzie più forti, ai sensi degli artt. 266 segg., in specie comma 2-*bis* c.p.p., per l'inserimento in specie del captatore informatico, nonché 266-*bis* c.p.p. per ogni "flusso" di comunicazioni informatiche e telematiche.

In queste tipologie di comunicazioni informatiche sfuma peraltro il carattere specificamente ed immediatamente "interpersonale" della riservatezza, la cui protezione si associa piuttosto a quella

della loro "sicurezza" rispetto ad attacchi cibernetici (*cybersecurity*, di cui sopra si è detto), del tutto eterogenei rispetto alle offese alle tradizionali forme di corrispondenza epistolare.

Tanto che appare necessario associare e collocare in questa sezione anche le norme penali poste genericamente a tutela dell'integrità dei dati e sistemi informatici, non caratterizzati da uno specifico significato o contenuto di "comunicazione" *fra persone*, ai quali va assicurata comunque una apposita tutela penale dell'integrità e della sicurezza informatiche, qual è quella offerta dall'incriminazione dei danneggiamenti informatici (artt. 635-*bis* segg. c.p.) e relative figure prodromiche (cfr. *infra* par. 4). Mentre rispetto ai "*documenti informatici*" strettamente intesi, caratterizzati da uno specifico "valore probatorio" nel traffico giuridico - di rilievo pubblico – deve valere la distinta disciplina penale delle falsità informatiche (art. 491-*bis* c.p.).

3.3.1. Proposta di introduzione del nuovo delitto di violazione della riservatezza delle comunicazioni informatiche

Previa abrogazione dell'ultima parte del comma 2 dell'art. 616 c.p., introdotta dalla legge 547/1993, la tutela penale delle comunicazioni informatiche deve essere specifica e più severa, rispetto a quella che è oggi assicurata genericamente alla corrispondenza cui quella "elettronica" era stata genericamente assimilata, richiedendo la previsione, all'interno della menzionata nuova "Sezione VI" del capo III del Titolo XII del Libro II del codice penale, del seguente nuovo delitto:

"*Violazione della riservatezza, disponibilità ed integrità delle comunicazioni informatiche*".

"*Chiunque senza autorizzazione intercetta, si procura, rende indisponibile ai legittimi destinatari od altera comunicazioni informatiche a lui non dirette o comunque a lui non rese disponibili da chi ha diritto di disporne, che abbiano un contenuto riservato, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni.*

Chiunque senza autorizzazione rivela, diffonde o rende comunque accessibile a terzi, anche mediante condivisione, riproduzione, messa a disposizione in rete, in tutto od in parte il contenuto delle comunicazioni informatiche di cui al primo comma, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a quattro anni.

Agli effetti della legge penale, per "comunicazioni informatiche" si intendono quelle effettuate con ogni mezzo o tecnica di trasmissione a distanza, compresa la condivisione, riproduzione o messa a disposizione di dati informatici, che rappresentino scritti, voci, suoni, immagini anche in movimento o altri contenuti che abbiano rilevanza per la comunicazione fra persone fisiche, giuridiche, enti e sistemi informatici.

Il delitto è punibile a querela della persona offesa".

La fattispecie, che semplifica e riorganizza l'ambito delle incriminazioni concernenti le comunicazioni informatiche aventi contenuto riservato, estrapolandole dai vigenti artt. 616 e 617-*ter* e seguenti c.p., ed in particolare assorbendo gli artt. 617-*quater*, 617- *quinquies* e 617-*sexies* c.p., punisce nel primo comma, innanzitutto, l'indebita "*intercettazione*" ed "*acquisizione*" con qualsiasi modalità tecnica, senza necessità che vi sia una "*presa di cognizione*" del contenuto da parte di una persona fisica; in secondo luogo l'"*alterazione*" del contenuto comunicativo riservato, veicolato dai dati informatici, qualsiasi natura o forma abbiano (di testo, audio, video, ecc.); infine il "*rendere indisponibili*" i menzionati contenuti, senza però che mai si richieda, per la consumazione, la causazione di un "*nocumento*" (come invece prevede l'attuale art. 616 c.p.) .

L'offesa alla riservatezza e alla sicurezza informatiche si consuma infatti già con la condotta tipica, che viola l'esclusività della conoscenza e disponibilità, ovvero l'integrità ed autenticità di detti dati, da parte di soggetti non destinatari o non altrimenti legittimati. All'acquisizione ed alterazione indebite è equiparato il fatto di rendere i dati informatici aventi tali contenuti "*indisponibili*" per il titolare, ad es. dislocandoli – anche mediante *software* c.d. maligni o *malware* - in spazi informatici a lui non accessibili ovvero con sistemi di criptazione abusivamente applicati.

Il secondo comma, in analogia con la struttura dell'art. 616 c.p. e di altre fattispecie poste a tutela dei segreti, prevede una fattispecie più gravemente sanzionata di "*rivelazione*" a terzi delle comunicazioni informatiche tutelate, peraltro ridefinendo il concetto, che non è più correlato ad una cognizione *personale* del contenuto da parte dell'autore, ma può avvenire direttamente con ogni mezzo o modalità tecnica automatizzata (ad es. mediante sistemi di intelligenza artificiale o *machine learning)*, compresa la diffusione o messa a disposizione di terzi in rete, e dunque senza (parziale o completa) presa di conoscenza del contenuto diffuso, essendo comunque l'aggravamento dell'offesa particolarmente rilevante nel *cyberspace*, le cui dimensioni spaziali e temporali rendono poi pressoché impossibile limitarne gli effetti.

La previsione, nei due commi, della clausola di illiceità speciale espressa dalla locuzione "*senza autorizzazione*" introduce un requisito oggettivo della fattispecie, che serve a circoscrivere la rilevanza penale alle condotte poste in essere senza legittimazione, a partire dall'assenza di consenso del titolare del diritto alla riservatezza o che non siano altrimenti permesse da specifiche disposizioni di legge o da provvedimenti dell'autorità ovvero anche da fonti private o negoziali: come nel caso invece di perquisizioni e sequestri da parte di agenti di polizia o di interventi autorizzati di servizi di sicurezza ovvero anche di operatori ed amministratori di sistema incaricati specificamente di interventi per rilevazioni e controlli della sicurezza, o nell'ambito di rapporti lavorativi o d'altro genere in cui questi siano contrattualmente consentiti.

Nel terzo comma si prevede una definizione espressa, agli effetti della legge penale, delle "*comunicazioni informatiche*" tutelate, che ne individui i tratti specifici, alla luce delle nuove tecnologie dell'informazione e della comunicazione nel *cyberspace*, in cui viene meno il carattere strettamente "*personale*" o meglio immediatamente "*interpersonale*" della comunicazione, che basta sia comunque "*riservata*" e come tale meritevole di protezione: carattere che può essere insito nell'essere una comunicazione veicolata, gestita, indirizzata da trattamenti automatizzati, compresi algoritmi e sistemi di intelligenza artificiale, non disponibili a terzi non legittimati.

Infine, il carattere del bene giuridico protetto, rappresentato dalla "riservatezza informatica" facente capo al titolare legittimato, con connessa sua disponibilità ed opportunità che sia lo stesso a valutare l'esigenza che sia o meno esercitata l'azione penale, consiglia di prevedere un regime di punibilità a querela di parte, che garantisca oltretutto il necessario filtro all'applicazione della fattispecie, evitando – dato il numero potenzialmente elevato di violazioni di questo tipo – di rendere problematica la possibilità di effettiva persecuzione da parte dell'Autorità giudiziaria e di gravarne eccessivamente l'attività.

4. I reati più specificamente offensivi della sicurezza informatica

4.1. Diffusione abusiva di dispositivi idonei a danneggiare un sistema informatico

La fattispecie di cui all'attuale art. 615-*quinquies* c.p., pur da mantenere, dovrebbe essere significativamente riformulata in conformità alle prescrizioni di fonte sovranazionale (ed in specie della direttiva 2013/40/UE) e ricollocata tra i reati contro la "*sicurezza informatica*", piuttosto che tra quelli contro la riservatezza informatica strettamente intesa: quindi subito dopo le fattispecie di danneggiamento di dati e di sistemi informatici (attuali artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p., da emendare e semplificare), in quanto è volta a punire comportamenti prodromici e preparatori rispetto alla consumazione di detti reati, anziché dell'accesso abusivo a sistemi informatici.

Art. 6 CoC	**Art. 7 Direttiva 2013/40/UE**
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: A the production, sale, procurement for use, import, distribution or otherwise making available of: ia device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences	Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and

established in accordance with Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor: (a)a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6; (b)a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Art. 615- *quinquies* c.p. ***Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico***	**Proposta di riforma** ***Produzione e diffusione abusiva di dispositivi idonei a danneggiare dati o sistemi informatici***
Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce,	**Salvo che il fatto costituisca più grave reato**[14], chiunque, allo scopo di danneggiare **senza autorizzazione dati o sistemi informatici**[15], ***abusivamente* produce**, procura **per sé o per altri**, riproduce, importa, diffonde, comunica, consegna o mette a disposizione di altri dispositivi, programmi

[14] La previsione di questa clausola di riserva ha lo scopo di evitare che il delitto prodromico e preparatorio in esame possa concorrere con le più gravi fattispecie in materia di danneggiamento di dati e di sistemi informatici.

[15] Pare opportuno, per ragioni di economia legislativa, semplificare la formulazione della fattispecie, sopprimendo il richiamo ai concetti di «*informazioni*» e di «*programmi informatici*», in quanto rientrano già in quello più ampio di «*dati informatici*» e limitando l'oggetto del dolo specifico al "*danneggiamento*" illecito di sistemi informatici o dei dati in essi contenuti, che abbraccia anche le ipotesi "speciali" di danneggiamento, che si sostanziano in una interruzione o alterazione del funzionamento di un sistema informatico.

importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.	informatici o **altri mezzi idonei a danneggiarli**[16], è punito con la reclusione fino a due anni e con la multa sino a euro 10.329. *Il delitto è perseguibile d'ufficio.*

4.2. La nozione di "*interferenze non autorizzate in ambito informatico*" (già impropriamente denominate "violenza informatica")

Il comma 3 dell'art. 392 c.p., aggiunto dalla legge 547/1993 alla fattispecie di esercizio arbitrario delle proprie ragioni mediante "*violenza sulle cose*", che al comma 2 già contiene la definizione ai fini penali di tale concetto generale, per la contingente volontà del legislatore di allora di estendere l'ambito del delitto ad ipotesi di alterazione strumentale di dati e programmi informatici, emerse in giurisprudenza e restate impunite per mancanza della qualità di "*cosa*" dei dati e del *software*, merita di essere riformulato e contraddistinto con una diversa denominazione ("*interferenze non autorizzate in ambito informatico*") da collocare, dopo i danneggiamenti informatici, fra i delitti contro la "*sicurezza informatica*".

Infatti, da un lato è bene che la nozione tradizionale di "*violenza sulle cose*", collegata strettamente alla materialità fisica del suo oggetto, non resti inquinata da elementi del tutto eterogenei; dall'altro, come la dottrina ha da tempo segnalato, va riconosciuto che un siffatto elemento si correla concettualmente alla nozione di danneggiamento, con la conseguenza che, diversificandosi questi strutturalmente, rispetto al tradizionale danneggiamento di cose (art. 635 c.p.), per adattarsi alla realtà dei "*dati e sistemi informatici*" che ne vanno a costituire i nuovi e diversi oggetti passivi, con correlata differenziazione delle relative fattispecie (artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p.), anche la nozione in esame deve rimodellarsi, per abbracciare tutti quegli interventi dannosi ed arbitrari su dati e *software*, che violino, oltre alla loro "*integrità*" strettamente intesa, anche la loro "*autenticità*", intesa come provenienza o riferibilità genuina al suo autore o titolare legittimo, nonché

[16] La vigente formulazione dell'art. 615-*quinquies* c.p. non richiede, sul piano oggettivo, l'intrinseca dannosità o pericolosità dei "dispositivi" che devono essere oggetto delle condotte di per sé "neutre" di *procurarsi*, *produrre*, *diffondere*, *importare*, *distribuire* o *cedere* suddetti oggetti materiali. Di conseguenza, il disvalore della norma incriminatrice viene a poggiare esclusivamente sul *fine illecito* che deve sorreggere il fatto-base. Onde evitare che vengano punite condotte prive di offensività oggettiva (ad es. chi consegna un programma informatico di per sé lecito al fine di commettere un danneggiamento di dati o di sistemi informatici) pare corretto richiedere, sul piano oggettivo, l'*idoneità* dei dispositivi a danneggiare dati o sistemi informatici, conservando però anche l'elemento finalistico, che serve a distinguere – nel caso di programmi e dispositivi c.d. *double use* – l'utilizzazione illecita da quella lecita (ad es. da parte di operatori di sistema che debbano testarne la sicurezza).

la loro "*funzionalità*", intesa come capacità di essere utilizzati ed operare in conformità alla loro destinazione e struttura tecnica.

L'importanza di un'adeguata definizione generale, da equiparare con apposita clausola alla "*violenza sulle cose*" che costituisce elemento di altri delitti, quali l'estorsione (art. 629 c.p.) o la turbata libertà dell'industria o del commercio (art. 513 c.p.), impone di preferire un'adeguata terminologia coerente con quella delle fonti sovranazionali (in specie nella direttiva 2013/40/UE).

"***Interferenze non autorizzate in ambito informatico***"

"*Agli effetti della legge penale, si considerano equivalenti alla violenza sulle cose, le interferenze non autorizzate in ambito informatico, consistenti nell'alterazione, modificazione, cancellazione, soppressione, introduzione o trasmissione di dati o programmi informatici o nel renderli altrimenti indisponibili, ovvero nell'impedire o ostacolare gravemente il funzionamento di un sistema informatico, in assenza di autorizzazione dell'avente diritto".*

5. La tutela penale dell'identità digitale

Il legislatore italiano, dopo anni di immobilismo di fronte all'esplosione di fenomeni connessi all' *identity theft* quali, ad esempio, il *phishing* o le c.d. frodi identitarie, è intervenuto con l'art. 9, co. 1, lett. a), della legge 15 ottobre 2013, n. 119, che ha convertito in legge, con modificazioni, il decreto-legge 14 agosto 2013, n. 93, ("*recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*") inserendo nell'art. 640-*ter* c.p. ("*frode informatica*") un nuovo comma, che sanziona la frode informatica commessa mediante sostituzione (*furto o indebito utilizzo*) «*dell'identità digitale in danno di uno o più soggetti*»[17].

5.1. Le principali criticità

a. *Formulazione tecnica delle "modalità di realizzazione" delle condotte tipiche*

Sollevano dubbi le questioni relative alla formulazione tecnica della fattispecie e all'assenza di una definizione di "identità digitale" che possa essere rilevante almeno agli effetti della legge penale.

Sembra opportuno evidenziare che in sede di conversione del decreto legge, il Parlamento, anziché adottare l'originaria locuzione «*se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti*», ha optato per quella: «*furto o indebito utilizzo*». L'espressione "furto"

[17] Si ritiene si tratti di una circostanza aggravante della frode informatica, argomentando sul tenore della disposizione, che utilizza i termini "*se il fatto è commesso con*", anziché "se il fatto *consiste* in", rinviando necessariamente al contenuto tipizzato nell'ipotesi base di cui al co. 1 dell'art. 640-*ter*.

d'identità digitale sembra richiamare (impropriamente) le condotte di sottrazione e impossessamento previste dall'art. 624 c.p., che sono tecnicamente riferite ad un oggetto fisico-materiale, espresso dal termine "cosa".

L'identità digitale, però, anche se non definita normativamente, è chiaramente da intendersi quale entità immateriale insuscettibile di sottrazione ed impossessamento fisico. Anche se fosse "incorporata" in un supporto informatico, sarebbe quest'ultimo a rappresentare l'oggetto - la *res* - del "furto", non l'identità come tale.

Proprio le difficoltà sorte nel definire l'"acquisizione abusiva" dell'identità digitale, ha portato il legislatore a fare riferimento, in settori *extra* penalistici, alla nozione di «*impersonificazione*», definita dall'art. 30-*bis* del d. lgs. 141/2010[18]. Anch'essa, però, ammesso che possa costituire un utile parametro ermeneutico di ordine sistematico, appare inidonea a chiarire la distinzione, introdotta dal legislatore penale, fra "furto" e "utilizzo indebito".

Nemmeno la condotta di "indebito utilizzo" è, infatti, di facile interpretazione. Se l'identità digitale costituisce un profilo abilitativo "personale" per la fruizione di (o l'accesso a) determinati spazi informatici o servizi nel *Cyberspace* – vale a dire attraverso i sistemi informatici ed Internet - il suo "utilizzo" appare confondersi con il "trattamento" di *dati personali*, di cui al Codice *privacy* (d.lgs. 196/2003, come modificato dal citato d.lgs. 101/2018 di adeguamento al Regolamento 2016/679/*UE*, c.d. GDPR)[19].

Potrebbe essere maggiormente coerente con le intenzioni del legislatore richiamare la distinzione tra *unauthorized access* (*accesso* non autorizzato a sistemi altrui / *possesso* non autorizzato di dati altrui) e *unauthorized use* (*uso* non autorizzato di dati altrui lecitamente posseduti) e, dunque, la nozione di «*sostituzione dell'identità digitale*» ne rappresenterebbe generalmente l'effetto o la conseguenza.

---

[18] Si tratta del decreto di attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonché' modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi. (10G0170) (GU n.207 del 4-9- 2010 - Suppl. Ordinario n. 212). L'art. 30 bis, co. 1, prevede che: "Ai fini del presente decreto legislativo per furto d'identità si intende: a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto; b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)".

[19] Infatti, ai sensi dell'art. 4, n. 2, del Regolamento europeo, il "*trattamento*" consiste in qualsiasi operazione od insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali od insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Tale nozione di "trattamento" è riferita però soltanto ai "dati personali". Ed occorre precisare che non sempre è a questi riconducibile l'identità digitale, in quanto essa potrebbe invece costituire una "misura di sicurezza" adottata per la "protezione" dei dati e dei sistemi. Un suo "indebito utilizzo", in tal caso, comporterebbe una – o costituirebbe un'attività prodromica alla – violazione delle misure di sicurezza per l'accesso al sistema o per l'acquisizione di dati e informazioni.

Seguendo questa impostazione ermeneutica il «*furto*» dovrebbe essere interpretato alla stregua di un'apprensione illecita dell'identità digitale altrui (o delle sue "componenti" essenziali come, ad es., nome utente e *password*), mentre l'«*indebito utilizzo*» dovrebbe essere inteso quale "uso abusivo" dell'identità digitale.

b. *L'assenza di una definizione di "identità digitale"*

In ogni caso, pur tentando con estrema difficoltà, con riferimento alle condotte tipiche, di fornire soluzioni interpretative nei limiti imposti dal divieto di estensione analogica *in malam partem*, rimane irrisolto il problema definitorio dell' «*identità digitale*», quantomeno ai fini penali, che potrebbe essere intesa, da un lato, in senso più o meno restrittivo, ossia quale "profilo abilitativo", "profilo riconoscitivo" o "credenziale di autenticazione"; dall'altro lato, potrebbe essere ricondotta nell'ambito del più complesso sistema di protezione dei "dati personali".

c. *Il bene giuridico protetto*

Un'ulteriore questione che fa emergere l'incriminazione del "furto o indebito utilizzo di identità digitale" è rappresentata dalla sua collocazione sistematica (al comma 3 dell'art. 640-*ter* c.p.), vale a dire quale ipotesi aggravata di frode informatica.

Sia che la si qualifichi quale mera circostanza aggravante, sia che si voglia parlare di autonoma ipotesi di reato, né la condotta di "furto", né quella di "indebito utilizzo" di identità digitale potrebbe da sola assumere rilevanza penale, essendo questa condizionata alla sussistenza anche di tutti gli altri elementi del "*fatto*" richiamato comunque dal comma 3, che determina, anche sul piano del contenuto dell'offesa tipica, la sua dimensione strettamente patrimoniale connotata dagli eventi consumativi dell'altrui danno con ingiusto profitto per sé od altri.

Appare evidente che la discussione sul bene giuridico protetto dall'incriminazione dell'illegittima acquisizione ed/od abusiva fruizione dell'identità digitale altrui non possa invece essere ridotta alla sola tutela del patrimonio, di fronte a fenomeni criminosi ormai estremamente diffusi, che vanno ben oltre le truffe e le frodi informatiche commesse attraverso l'abuso di identità digitale.

Ulteriori e gravi profili d'offesa di diritti anche fondamentali ed interessi meritevoli di protezione (penale) nel *Cyberspace* sono ravvisabili in tali fenomeni, a partire dalle conseguenze anche psicologiche sofferte dalle vittime[20], fino all'eventuale pregiudizio all'onore ed alla reputazione subìto dalla persona offesa[21], in ogni caso potendo essere coinvolte lesioni alla sfera più intima della riservatezza e dell'autodeterminazione informativa[22], accanto a profili di sicurezza e di certezza nel

[20] Si pensi all'abuso di identità digitale che comporti il caricamento, su canali personali di social media o social network, di video a sfondo sessuale che vedono come protagonista la persona offesa.
[21] Si pensi alle ipotesi di abuso di identità digitale con cui vengono caricati, ad es. sul profilo personale di Facebook, frasi offensive, ovvero post con contenuti razzisti o aventi ad oggetto diverse forme di apologia.
[22] Si fa riferimento ai casi in cui l'abuso dell'identità digitale comporta l'accesso a spazi informatici riservati, contenenti dati personali, se non intimi o segreti.

traffico giuridico informatizzato, di interesse di tutta la collettività nell'attuale dimensione globale della Rete.

5.2. Proposte di riforma

L'identità digitale (ID)

Ai fini dell'introduzione di una definizione di identità digitale (postea: ID) ai fini penali è opportuno, preliminarmente, delinearne i tratti caratteristici sul piano tecnico-informatico.

a. *Oggetto dell'ID*

L'ID "rappresenta" un soggetto, persona fisica o giuridica, ovvero un *device,* un applicativo o un sistema (postea: *user*) nelle interrelazioni che si realizzano nel *cyberspace* o, più in generale, nel contesto tecnologico, nell'ambito dei rapporti uomo-macchina e macchina-macchina nella comunicazione mediata dal *computer* [*computer mediated communication* (CMC)].

b. *Le funzioni dell'ID*

L'ID nella CMC svolge diverse funzioni.

b.I. La funzione identificativa

L'ID ha anzitutto lo scopo di identificare in modo univoco l'*user* nelle CMCs, ovvero nei rapporti anzidetti, attraverso l'attribuzione di credenziali o profili riconoscibili dal sistema informatico (inteso in tutte le sue componenti *hardware* e *software*), ovvero tramite l'incorporazione di caratteristiche di riconoscimento personale.

b.II. La funzione autenticativa

L'ID consente di attivare un processo di autenticazione da parte del sistema, che riconosce in tal senso l'*user* quale soggetto legittimato ad accedere e ad operare attraverso le sue risorse (c.d login).

b.III. La funzione autorizzativa e di controllo

L'*user*, una volta autenticato, è autorizzato a svolgere determinate operazioni o ad accedere ad aree informatiche sulla base di diversi profili di autorizzazione attribuiti dal titolare del sistema o dal sistema medesimo.

c. *Gli "strumenti" dell'ID*

L'*user* può essere identificato attraverso l'attribuzione di credenziali identificative, abilitative e autorizzative di diverso tipo: nome utente e *password*, tessere magnetiche, *smart card*, informazioni biometriche (iride, impronta digitale, impronta vocale, riconoscimento del volto), codici binari o identificativi di *device* (ad esempio anche il semplice *IP address* potrebbe consentire e autenticare l'accesso, nonché l'utilizzo di determinati sistemi in base al riconoscimento del *device* o della rete di "provenienza"), combinazioni multi-fattoriali (ad es. *smart card* e impronta digitale). Si pensi, per

ipotesi, anche alla Carta d'identità elettronica italiana e alla Carta nazionale dei servizi, che costituiscono strumenti di autenticazione previsti dal Codice dell'Amministrazione Digitale per l'accesso ai servizi web erogati dalle Pubbliche Amministrazioni.

Proposta di formulazione di una nuova fattispecie penale

a. *Collocazione sistematica*

Abrogazione del co. 3 dell'art. 640 ter c.p.

Introduzione, a chiusura della nuova Sezione VI, dedicata ai "*Delitti contro la riservatezza e la sicurezza informatica*" (del Capo III del Titolo XII), di un nuovo autonomo delitto denominato:

Abuso di identità digitale, avente la seguente:

b. *Formulazione tecnica*

«*Salvo che il fatto costituisca più grave reato, chiunque senza autorizzazione crea o procura per sé o per altri, ovvero utilizza, riproduce, comunica, consegna, cede a qualsiasi titolo, mette a disposizione del pubblico o diffonde dati, informazioni, programmi, ovvero ogni altro applicativo, che consentono di rappresentare un'identità digitale , è punito con la reclusione da sei mesi a due anni e con la multa fino a quindicimila euro.*

Il delitto è punibile a querela della persona offesa, salvo non ricorrano taluna delle circostanze aggravanti di cui al secondo, terzo e quarto comma dell'art. 615-ter c.p., o nei casi in cui il fatto riguardi una rilevante quantità o un rilevante numero di identità digitali.

Ai fini della legge penale si intende per identità digitale qualsiasi dato, informazione, codice, programma, applicativo o supporto, anche in combinazione fra di loro, che consentano l'individuazione, il riconoscimento o l'autenticazione di una persona fisica o giuridica nella interazione con i sistemi informatici o telematici ovvero per l'accesso ad essi o per la fruizione di servizi o funzioni tramite essi offerti».

c. *Sintesi delle motivazioni e bene giuridico protetto*

La formulazione proposta permette di superare le criticità evidenziate con riferimento alla previsione attuale relegata all'ipotesi aggravata di frode informatica. L'identità digitale è definita, ai fini della legge penale, quale entità immateriale, che comprende molteplici connotazioni e contenuti tecnici (dati, informazioni, programmi, supporti), i quali non necessariamente integrano o sono assorbiti nella nozione di "*dato personale*" ai sensi del Regolamento 2016/679/ UE (GDPR), perché possono riferirsi anche ad un mero "*dispositivo*".

In secondo luogo, la precisa individuazione delle condotte penalmente rilevanti consente, da un lato, di evitare le insidiose difficoltà ermeneutiche che nascono nell'interpretazione dei concetti di

"*furto*" e di "*indebito utilizzo*" e, dall'altro lato, di tenere distinta la tutela penale dell'identità digitale dalla disciplina dei dati personali, con cui potrebbe rischiare altrimenti di confondersi.

In terzo luogo, la tutela penale dell'identità digitale assume rilevanza autonoma, non più limitata alla dimensione patrimoniale della frode informatica, rispondendo alle attuali esigenze di protezione da fenomeni criminosi ormai estremamente diffusi, che recano offesa a diritti fondamentali della persona e ad ulteriori interessi meritevoli di tutela penale nel *cyberspace*: dalla sfera più intima della riservatezza personale all'autodeterminazione informativa, dalla sicurezza e certezza nel traffico giuridico informatizzato, all'interesse di tutta la collettività all'identificazione corretta dei soggetti che operano nell'attuale dimensione globale della Rete.

Con riferimento all'aspetto sanzionatorio, la natura e gravità della pena detentiva si allinea a quella dei delitti collocati nella Sezione in questione, prevedendosi anche una pena pecuniaria congiunta, data la rilevanza anche economica che potenzialmente o concretamente riveste il reato.
Alla luce della nuova formulazione e collocazione sistematica, è comunque configurabile un concorso con altri reati, a partire da quello con la frode informatica di cui all'art. 640-*ter* c.p., nel cui ambito è oggi restrittivamente collocata.

Testo sintetico dell'articolato proposto

[CAPO III
Dei delitti contro la libertà individuale]

Sezione VI
Dei delitti contro la riservatezza e la sicurezza informatiche

Accesso non autorizzato ad un sistema informatico

[I] Chiunque accede senza autorizzazione o eccedendone i limiti ad un sistema informatico o ad una sua parte è punito con la reclusione fino a tre anni.

[II] La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di amministratore od operatore di sistema;

2) se il colpevole commette il fatto mediante interferenze informatiche

3) se il fatto è commesso nell'ambito di una associazione per delinquere

[III] Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici di pubblica utilità o di una infrastruttura critica, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

[IV] Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Produzione e diffusione abusiva di codici di accesso ad un sistema informatico

[I] Fuori dai casi previsti dall'articolo precedente, chiunque, al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno, abusivamente produce, procura per sé o per altri, riproduce, diffonde, comunica o consegna codici, *password*, dati informatici o altri mezzi idonei

all'accesso abusivo ad un sistema informatico, è punito on la reclusione sino a due anni e con la multa sino a euro 10.329.

[II] La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 15.492 se ricorre taluna delle circostanze di cui al secondo e terzo dell'art. 615-ter c.p.

Violazione della riservatezza, disponibilità ed integrità delle comunicazioni informatiche

Chiunque abusivamente intercetta, si procura, rende indisponibile ai legittimi destinatari od altera comunicazioni informatiche a lui non dirette o comunque a lui non rese disponibili da chi ha diritto di disporne, che abbiano un contenuto riservato, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni.

Chiunque abusivamente rivela, diffonde o rende comunque accessibile a terzi, anche mediante condivisione, riproduzione, messa a disposizione in rete, in tutto od in parte il contenuto delle comunicazioni informatiche di cui al primo comma, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a quattro anni.

Agli effetti della legge penale, per comunicazioni informatiche si intendono quelle effettuate con ogni mezzo o tecnica di trasmissione a distanza, compresa la condivisione, riproduzione o messa a disposizione di dati informatici, che rappresentino scritti, voci, suoni, immagini anche in movimento o altri contenuti che abbiano rilevanza per la comunicazione fra persone fisiche, giuridiche, enti e sistemi informatici.

Il delitto è punibile a querela della persona offesa.

Danneggiamento di dati informatici

[I] salvo miglior formulazione: [Artt. 635-bis e 635-quater c.p.]

Danneggiamento di sistemi informatici

[I] salvo miglior formulazione: [Artt. 635-ter e 635-quinquies c.p.]

Interferenze non autorizzate in ambito informatico

Agli effetti della legge penale, si considerano equivalenti alla violenza sulle cose, le interferenze non autorizzate in ambito informatico, consistenti nell'abusiva alterazione, modificazione, cancellazione, soppressione, introduzione o trasmissione di dati informatici o nel renderli altrimenti indisponibili, ovvero nell'impedire o ostacolare gravemente il funzionamento di un sistema informatico

Produzione e diffusione abusiva di dispositivi idonei a danneggiare dati o sistemi informatici

[I] Salvo che il fatto costituisca più grave reato, chiunque, allo scopo di danneggiare senza autorizzazione dati o sistemi informatici, abusivamente produce, procura per sé o per altri, riproduce, importa, diffonde, comunica, consegna o mette a disposizione di altri dispositivi, programmi informatici o altri mezzi idonei a danneggiarli, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

[II] La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 15.492 se ricorre taluna delle circostanze di cui al secondo e terzo dell'art. 615-ter c.p.

Abuso di identità digitale

[I] Salvo che il fatto costituisca più grave reato, chiunque abusivamente crea o procura per sé o per altri, ovvero abusivamente utilizza, riproduce, diffonde, comunica o consegna dati o programmi che consentono di rappresentare un'identità digitale altrui, è punito con la reclusione da sei mesi a due anni e con la multa fino a quindicimila euro. Il delitto è punibile a querela della persona offesa, salvo non ricorrano taluna delle circostanze aggravanti di cui al secondo, terzo e quarto comma dell'art. 615-ter c.p.

[II] Ai fini della legge penale si intende per identità digitale qualsiasi dato, informazione, codice, programma, applicativo o supporto che consentano l'individuazione, il riconoscimento o l'autenticazione di una persona fisica o giuridica, ovvero di un qualsiasi dispositivo per la interazione con un programma, una banca dati od un sistema informatico, o per l'accesso ad essi ovvero per la fruizione di servizi o funzioni da essi offerti.