Digeat N.5 - 19 Marzo 2025

# I dati e l’identità digitale: aspetti di diritto penale

*Di Giovanni Fiorino*

## Abstract

Il contributo si propone di esaminare gli effetti della diffusione delle nuove tecnologie nel settore delle condotte penalmente rilevanti, nel rispetto dei principi di tassatività e non indeterminatezza della fattispecie penale. In tale prospettiva, viene esaminata l’evoluzione giurisprudenziale in ordine all’applicazione delle norme di diritto penale alle condotte poste in essere mediante strumenti informatici e telematici, con specifico riferimento agli articoli 595 c.p. (Diffamazione) e 494 c.p. (Sostituzione di persona): l’accertamento della condotta criminosa ha determinato anche lo sviluppo di nuovi strumenti d’indagine e di prova determinati dalle caratteristiche informatiche e telematiche delle circostanze di fatto rilevanti ai fini della riconducibilità della condotta stessa ad una persona fisica. Lo sviluppo delle forme di criminalità informatica, ed in particolare degli attacchi informatici, ha portato all’approvazione della legge n. 90/2024, che contiene anche rilevanti modifiche al codice penale e, in particolare, la creazione della fattispecie di reato della “estorsione informatica” (art. 629 comma 3 c.p.) nell’ambito della quale è possibile ricondurre la condotta tecnicamente nota con il nome di “ransomware”.

## Indice



## Identità digitale ed anonimato nel sistema penale: autore e persona offesa nei reati informatici

La diffusione capillare della navigazione Internet ha posto sin da subito, accanto alle innegabili opportunità, le questioni inerenti alla possibilità che, mediante tale navigazione, venissero commessi atti illeciti anche costituenti reato.

In particolare, si è discusso a lungo non solo in merito alle nuove condotte potenzialmente idonee a ledere beni giuridici di particolare rilievo e, come tali, degni di protezione anche mediante la previsione di **nuove fattispecie di reato calibrate sull’utilizzo delle tecnologie,** ma anche in merito alla **difficile identificabilità dell’autore della condotta illecita**, mascherato dietro un personal computer mediante il quale tale condotta ha leso o messo in pericolo i predetti beni giuridici.

A ciò deve aggiungersi che la navigazione sulla rete Internet è stata vista, sin da subito, come un **modo per raccogliere dati** riguardanti le preferenze dell’autore della navigazione stessa, le sue

ricerche e i suoi interessi, così da permetterne una **profilazione idonea** a consentire non solo l'invio di messaggi promozionali calibrati proprio su quegli interessi, ma anche **la commercializzazione del profilo del navigatore**, messo a disposizione di soggetti interessati a sfruttarne le potenzialità.

> In tale prospettiva si è sviluppato da un lato il dibattito sulla tutela della "navigazione anonima" e, dall'altro, quello sulla necessità di superare l'anonimato in vista della protezione di interessi particolarmente rilevanti quali, appunto, quelli connessi alla prevenzione e punizione di condotte penalmente illecite.

**Il diritto alla protezione dell'anonimato**, di cui all'articolo 10 della Dichiarazione dei Diritti di Internet, è stato definito il diritto a che tutti gli ordinamenti giuridici permettano agli individui di svolgere attività in rete senza l'obbligo di identificarsi con precisione.

Esso è articolato in **tre punti essenziali,** in particolare: che ogni persona possa accedere alla rete e comunicare elettronicamente, usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali anche per **esercitare le libertà civili e politiche senza subire discriminazioni o censure**; che le limitazioni a questo tipo di anonimato dovrebbero poter essere previste solamente quando siano giustificate dall'esigenza di tutelare rilevanti interessi pubblici e risultino necessarie, proporzionate, fondate sulla legge e nel rispetto dei caratteri propri di una società democratica; che, nei casi di violazione della dignità e dei diritti fondamentali, l'Autorità giudiziaria, con **provvedimento motivato**, dovrebbe poter disporre l'identificazione dell'autore della comunicazione[1] .

> Pertanto, accanto all'esigenza di tutela dell'anonimato, si rinviene quella di garantire l'identificazione dell'autore della condotta al fine di assicurare la salvaguardia di rilevanti interessi pubblici.

Com'è noto, tale identificazione presenta delle **difficoltà peculiari** connesse all'utilizzo di strumenti informatici e telematici: internet è una rete di macchine collegate fra di loro e, quindi, **ciò che andrà identificato sarà *in primis* la macchina** (il computer) da cui è partita l'azione ed il secondo passo consisterà nel **collegare il computer "incriminato" alla persona fisica** (l'utente) che materialmente ha commesso la condotta criminosa servendosi della macchina stessa.

In tale contesto, assume rilievo l'identificazione dell'utente mediante la individuazione **dell'indirizzo IP dinamico**, attribuitogli temporaneamente per il periodo in cui egli è connesso: il primo passo verso la predetta identificazione sarà quindi conoscere l'IP del computer utilizzato[2].

Nell'ottica del contemperamento tra **esigenze di riservatezza dei dati** (anche inerenti la navigazione in rete) e tutela di interessi giuridici rilevanti, è stata **disciplinata la conservazione e la messa a disposizione** delle informazioni riguardanti la connessione Internet dei singoli utenti, ovvero **la "*data retention*",** da intendersi quale periodo di conservazione dei dati elettronici o analogici[3]: tra le informazioni rilevanti vi è, appunto, quella relativa all'assegnazione dell'indirizzo IP con contestuale possibilità di ricondurre detto indirizzo all'utenza telefonica e, dunque, ad una persona fisica potenzialmente coinvolta nell'attività illecita.

La disciplina è contenuta nell'articolo 132 del decreto legislativo n. 196/2003, articolo rubricato **"Conservazione di dati di traffico per altre finalità"**, che, al primo comma, così dispone: "Fermo restando quanto previsto dall'articolo 123, comma 2 […] per finalità di accertamento e repressione dei reati […] i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione".

> Il "navigatore" della rete internet può essere "persona offesa", destinataria di condotte illecite: in tale prospettiva l'anonimato rappresenta una modalità "virtuosa" grazie alla

> quale l’utente è tutelato rispetto ad attività di profilazione non desiderate.

D’altro canto, però, la sua identità reale può essere oggetto di aggressioni penalmente rilevanti: si pensi, ad esempio, al **delitto di diffamazione “on line**”, che rientra nella fattispecie di cui all’articolo 595 comma 3 c.p.[4], ovvero a quello di **sostituzione di persona** mediante la creazione di account di posta elettronica o profili social network che riconducono l’identità digitale a persone fisiche del tutto estranee all’account o al profilo creato[5].

Le aggressioni da remoto a beni giuridici rilevanti possono determinare anche **un aggravamento del trattamento sanzionatorio,** in considerazione della conseguente “minorata difesa” della vittima del reato: difatti la norma di cui all’articolo 61 n. 5 c.p. – “l’avere profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all’età, tali da ostacolare la pubblica o privata difesa” – altresì richiamata dall’articolo 640 comma 2 bis c.p., è stata ritenuta applicabile alle ipotesi di truffa “on line” posto che, sin dalle prime pronunce sul punto, la Corte di Cassazione ha rilevato che “Proprio [la] distanza tra il luogo di commissione del reato da parte dell’agente e il luogo dove si trova l’acquirente è l’elemento che consente all’autore della truffa di porsi in una situazione di maggior favore rispetto alla vittima, di schermare la sua identità, di fuggire comodamente, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell’acquirente”[6]

## Tutela della identità della persona offesa dal reato ed esigenza di identificazione dell’autore della condotta criminosa nella legge n. 90/2024

Con la legge n. 90/2024, il legislatore ha disciplinato la **materia degli attacchi informatici** e, in tale contesto, hanno trovato sede anche modifiche rilevanti al codice penale: difatti, in taluni casi, l’aver commesso il fatto/reato “a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione” (articolo 640 comma 2 ter c.p.) costituisce una circostanza aggravante la cui ratio è da rinvenire nella **maggiore severità sanzionatoria nei confronti di chi ha operato in modo da celare la propria identità**; in altri casi, “l’inaccessibilità, al legittimo titolare, dei dati o dei programmi informatici” (articolo 615 ter comma 2 n. 3 ultima parte c.p. o, ancora, articolo 635 ter comma 3 n. 3 c.p.) costituisce circostanza aggravante funzionale ad una maggiore severità della pena verso chi ha violato l’altrui identità digitale impedendo al titolare di accedere al patrimonio informativo costituito da dati, informazioni e programmi.

> Nella prospettiva appena delineata assume particolare rilevanza la norma dell’articolo 629 c.p. il cui terzo comma, inserito proprio dall’articolo 16 comma 1 lettera m) della legge n. 90/2024, punisce la condotta estorsiva commessa mediante l’accesso abusivo al sistema informatico o telematico (art. 615 ter c.p.), mediante l’intercettazione, l’impedimento o l’interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.), mediante la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.), mediante il danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.), mediante il danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) ovvero il danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635 quinquies c.p.).

Anche la sola minaccia di compiere le predette condotte è sufficiente ad integrare la fattispecie di reato.

Si tratta del reato definito, in gergo, “estorsione informatica”.

## Estorsione informatica e ransomware: il nuovo articolo 629 comma 3 c.p.

Nell'ambito degli attacchi informatici maggiormente diffusi ed aggressivi, quello immediatamente riconducibile alla fattispecie di cui all'articolo 629 comma 3 c.p. è il "**ransomware**", software malevolo, cosiddetto malware, il quale, una volta aperto, cifra i dati rendendo i file dell'utente danneggiato inutilizzabili.

> Solitamente, il ransomware viene attivato aprendo il file che lo contiene, cosicché esso procederà alla cifratura dei dati della vittima quali, ad esempio, documenti, immagini e ogni altra informazione contenuta nel computer. Ciò che caratterizza questo malware è la condotta del criminale che chiederà un riscatto alla vittima perché la stessa possa riavere i file decriptati e utilizzabili nuovamente[7].

Gli aspetti del malware rilevanti, nella prospettiva di cui al novellato articolo 629 c.p., riguardano la **inutilizzabilità** dei dati dell'utente, mediante la **cifratura** degli stessi, e la richiesta del **riscatto** al fine di consentire la **decriptazione** dei dati: in tale prospettiva, assumono particolare rilievo, fra le disposizioni normative richiamate dalla norma dell'articolo 629 comma 3 c.p., quelle che **puniscono il danneggiamento dei dati stessi** (art. 635 bis c.p.) ovvero il **danneggiamento dei sistemi informatici o telematici**, anche di pubblico interesse mediante la consumazione delle condotte punite dall'articolo 635 bis c.p. (artt. 635 quater e 635 quinquies c.p.)

Delineato l'ambito normativo di riferimento, è necessario individuare la condotta punita dall'articolo 635 bis c.p., descritta quale **distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi**: in particolare, occorre verificare se l'attività tecnico informatica della "cifratura dei dati" – caratteristica del ransomware – rientri nella condotta tipizzata dal richiamato articolo 635 bis c.p.

> Sul punto, è necessario ricordare che, secondo l'interpretazione consolidata della giurisprudenza di legittimità, il "danneggiamento informatico" è ravvisabile in caso di cancellazione di file da un sistema informatico sia quando la cancellazione sia stata provvisoria, mediante lo spostamento dei files nel cestino, sia quando la cancellazione sia stata definitiva, con il successivo svuotamento del cestino, essendo comunque irrilevante che anche in tale ultima evenienza i files cancellati possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze nel campo dell'informatica[8].

In particolare, nella motivazione della sentenza n. 8555/2011, la Corte di Cassazione ha precisato che "il lemma cancella che figura nel dettato normativo non può essere inteso nel suo precipuo significato semantico, rappresentativo di irrecuperabile elisione, ma nella specifica accezione tecnica recepita dal dettato normativo, notoriamente introdotto in sede di ratifica di Convenzione Europea in tema di criminalità informatica (con L. 23 dicembre 1993, n. 547)".

Sul punto, la Corte ha sottolineato che "nel gergo informatico, l'operazione della cancellazione consiste nella rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via «definitiva» mediante il successivo svuotamento dello stesso. L'uso dell'inciso per evidenziare il termine «definitiva»", prosegue la Corte, "è dovuto al fatto che neppure tale operazione può definirsi davvero tale, in quanto anche dopo lo svuotamento del cestino i files cancellati possono essere recuperati, ma solo attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze nel campo dell'informatica".

Pertanto, la Corte ha concluso affermando che "sembra corretto ritenere conforme allo spirito della disposizione normativa che anche la cancellazione, che non escluda la possibilità di recupero se non

con l'uso – anche dispendioso – di particolari procedure, integri gli estremi oggettivi della fattispecie delittuosa".

In tale prospettiva, è possibile affermare che **la criptazione dei dati informatici**, rendendo gli stessi temporaneamente non accessibili all'utente, **rientri nel significato non semantico, ma tecnico del termine "cancellazione"** adoperato dal legislatore nell'articolo 635 bis c.p. e, dunque, che la condotta che caratterizza il fenomeno del ransomware rientri nella fattispecie di reato della "estorsione informatica" delineata dalla norma dell'articolo 629 comma 3 c.p. introdotta dalla legge n. 90/2024.

## Conclusioni

La dimensione digitale dei dati e della identità costituisce uno degli aspetti più rilevanti dell'impatto delle nuove tecnologie nella vita privata, ma anche dello svolgimento di attività commerciali e di rilevanza pubblica: dalla tutela del domicilio informatico, protetto dalla norma dell'articolo 615 ter c.p., si è passati alla tutela dell'identità, oggetto specifico dei diritti sanciti dall'articolo 9 della Convenzione dei diritti di Internet e che, per quel che attiene al presente studio, è da intendersi quale diritto di ogni persona "alla rappresentazione integrale e aggiornata delle proprie identità in rete" e la cui definizione "riguarda la libera costruzione della personalità" non sottratta all'intervento e alla conoscenza dell'interessato[9].

A ciò si aggiunga che anche **il fenomeno criminale degli attacchi informatici, in genere, e del "ransomware", in particolare, è in continua evoluzione**: l'analisi degli aspetti tecnici costituisce un momento di assoluto rilievo poiché essa consente di individuare la "condotta" penalmente rilevante e di verificare in che termini la stessa, nel rispetto del **principio di tassatività** e **non indeterminatezza** della fattispecie penale, può essere inquadrata esattamente nell'ambito della norma giuridica, generale ed astratta, ovvero necessita di un intervento normativo che, date le peculiarità del fenomeno criminale, non può che **attingere anche ad esperienze di altri Paesi** così da consentire la realizzazione di un quadro normativo coerente.

---

**NOTE**

[1] Giovanni Ziccardi, Anonimato (Diritto all') in AAVV, Dizionario Legal Tech a cura di Giovanni Ziccardi e Pierluigi Pierri, Milano, 2020, pagg. 37 ss

[2] F. Boezio, M. D'Alessio, Internet e responsabilità penali, in AAVV, Internet e responsabilità giuridiche a cura di Giuseppe Vaciago, Piacenza, 2002, pagg. 306 ss.

[3] L. Piatti, voce "Data retention", in AAVV, Dizionario Legal Tech, cit., pagg. 305 ss.

[4] Per il consolidato orientamento giurisprudenziale che ritiene che la pubblicazione sulla rete internet o sui social network di affermazioni lesive dell'onore e della reputazione altrui rientranti nella fattispecie di cui all'articolo 595 c.p. cfr. Corte di Cassazione, sentenza n. 4741/2000 nonché Corte di Cassazione, sentenza n. 16262/2008 con specifico riferimento all'operatività della condotta nel'ambito dei social network ed infine Corte di Cassazione, sentenza n. 13979/2021 in merito alla circostanza aggravante di cui all'articolo 595 comma 3 c.p.. Per gli aspetti inerenti la identificazione dell'autore del reato mediante l'indirizzo cfr. Corte di Cassazione, sentenza n. 8824/2010; per la rilevanza di altri elementi di prova oggetto dell'istruzione dibattimentale, aventi ad oggetto l'attribuzione all'imputato del contenuto diffamatorio, in caso di mancata identificazione dello stesso mediante indirizzo IP, cfr. Corte di Cassazione, sentenza n. 5352/2017

[5] Corte di Cassazione, sentenza n. 12479/2011; v. anche Corte di Cassazione, sentenza n. 42572/2018 che riguarda il caso specifico della iscrizione ad un sito di e-commerce servendosi dei dati anagrafici di un diverso soggetto  con il fine di far ricadere su quest'ultimo l'inadempimento delle obbligazioni conseguenti all'avvenuto acquisto di beni; Corte di Cassazione, sentenza n. 22049/2020 (Fattispecie relativa alla creazione di falsi profili "facebook")

[6] Corte di Cassazione, sentenza n. 43705/2016. Sul punto cfr. più di recente, Corte di Cassazione, sentenza n. 18252/2002 che conferma l'orientamento giurisprudenziale.

[7] Andrea Scirpa, voce "Ransomware" in Dizionario Legal Tech, cit., pagg. 798 s.

[8] Corte di Cassazione, sentenza n. 8555/2011.

[9] G. Ziccardi, voce "Identità" in AAVV, Dizionario Legal Tech, cit. pagg. 513 ss