di Giuseppe Specchio

ANALISI DI CONTESTO DEL CYBERSPACE (I PARTE)

Giuseppe SPECCHIO, Ufficiale dell'Arma dei Carabinieri, specialista in Informatica Forense presso il Raggruppamento Operativo Speciale Carabinieri (ROS). Svolge con assiduità un'attività di docenza presso l'Istituto Superiore Tecniche Investigative dell'Arma dei Carabinieri in Velletri ove presenta casi investigativi reali opportunamente anonimizzati e risolti con strumentazione prevalentemente Open Source.

Il presente articolo è stato redatto con l'obiettivo di fornire: una definizione formale ed esaustiva del cyberspace; una descrizione delle principali fonti del diritto e degli elementi costitutivi del ***cyberspace***, soffermandosi in modo particolare sui dei soggetti attivi e delle condotte antigiuridiche da essi assunte, nonché i soggetti terzi che assumono il ruolo ***"legittimo titolare"*** (o ***lawful authority***) così come sancito dall'art. 234 ***bis*** c.p.p.; una descrizione delle principali difficoltà tecnico-operative, anche alla luce delle imminente entrata a regime della triade IoT, 5G ed Intelligenza Artificiale; proporre un ***workflow*** investigativo in tale ambito.

In questo numero: 1. Cosa si intende per Cyberspace, 2. I principali elementi costitutivi del cyberspace, 2.a. Le fonti del diritto, 2.b. La figura del "legittimo titolare", 2.c. La nozione di reato informatico.

Nel prossimo numero: 2.d. I soggetti attivi del cyberspace, 2.e. Difficoltà nell'identificazione del contratto di utenza residenziale o mobile. 3. L'attuale contesto operativo, 4. Conclusioni.

1. Cosa si intende per *Cyberspace*

Attualmente non esiste una definizione legale ed universalmente riconosciuta di *cyberspace*, anche perché gli ordinamenti giuridici coinvolti sono diversi tra loro. Per tale motivo, possiamo ristringere tale nozione solo al dominio tecnico, così come raccomandato dalla ISO 27032:2012[1], secondo la quale viene definito come ***cyberspace*** (o ciberspazio):

«the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form»

ossia un ambiente virtuale (o totalmente dematerializzato) definito dal:

«complesso delle attività realizzate dai soggetti che usufruiscono dei servizi offerti dalla rete Internet attraverso l'impiego di sistemi informatici e telematici[2] ad essa collegati».

1 http://www.iso27001security.com/html/27032.html

2 Corte di Cassazione (Sez. VI n. 3067 del 14.12.1999; Sez. V n. 31135 del 6.7.2007)

«… deve ritenersi "sistema informatico", […] , un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla

È di fatto un ambiente *"incoercibile"* nella sua interezza, in quanto, per sua natura, la sovranità di uno Stato (o *domestic jurisdiction*)[3] può essere esercitata solo nei luoghi di partenza o di arrivo delle comunicazioni elettroniche *"fisicamente"* e legalmente presenti nella sfera di controllo del singolo Stato.

La nozione di *"territorio"* è stravolta, in quanto stiamo parlando di un contesto operativo tendenzialmente *"deperimetralizzato"* e *"liquido"*, caratterizzato da:

- un **azzeramento**, di fatto, **delle distanze**, valutabili al massimo in termini di *hop* (o salti)[4];
- un'**ubiquità** di accesso alle risorse distribuite (es. si pensi alla possibilità di accedere contemporaneamente, con più sistemi informatici, ad un foglio elettronico di *Google Docs*);
- una **ridondanza informativa**, ossia se non posso accedere ad uno *smartphone* perché non siamo a conoscenza del suo codice di sblocco, l'investigatore potrebbe accedere ad una copia (totale o parziale) dei dati di interesse per le indagini presenti su un altro supporto (es. un *cloud storage*);
- **multidentità** ed **anonimizzazione** dei cibernauti, ossia l'esistenza di un rapporto 1:N tra l'identità reale e quelle virtuali, le quali possono essere gestite contemporaneamente, ancorché con veri e propri *"passamontagna virtuali"*. A tale risultato si giunge anche grazie a dei vincoli sia tecnici che giuridici, come ad esempio:
  - un collegamento ad un *social network* mediante l'intermediazione di uno o più *proxy server*, i quali consentono di dissimulare la propria presenza in Rete, la cui identificazione viene ulteriormente complicata se si cifra l'intero canale di comunicazione (es. mediante una VPN[5]);
  - un disallineamento delle norme internazionali in materia di contrasto ai *cybercrime* (*cfr.* § par. 3.c - Si considerino, ad esempio, gli effetti collaterali, in termini investigativi, della *data retention*[6], dell'uso del NAT[7] da parte degli *access provider*[8], dell'impiego dei *"Proxy Registration Service"*[9]);
  - complicanze derivate dall'attuazione di norme comunitarie, come ad esempio il GDPR (*General Data Protection Regulation*)[10], che, a partire dal 25 maggio 2018, ha di fatto snaturato la natura del servizio pubblico di Whois[11], costringendo così le autorità giudiziarie all'adozione di misure di cooperazione internazionale anche per avere informazioni, ancorché poco attendibili, nonostante gli sforzi profusi da ICANN[12], sui Registrants (intestatari dei nomi di dominio)[13];
  - assenza di cooperazione internazionale tra gli Stati interessati.
- un conseguente e tendenziale **abbassamento dei freni inibitori** (es. *sexting*[14]) e della sensazione di punibilità (es. *cyber stalking*);
- un ***"diritto all'oblio"***[15] ridotto ai minimi termini, in virtù dell'impossibilità tecnica, in termini assoluti, di *"confiscare e distrug-*

"registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente ...».

«… è "sistema telematico" l'insieme di più sistemi informatici collegati tra loro per lo scambio di informazioni, purché siano connessi in modo permanente, e purché lo scambio di informazioni sia il mezzo necessario per conseguire i fini operativi del sistema. ...»

3 Con il termine **sovranità** (o *domestic jurisdiction*) s'intende la capacità di un ente (Stato) di:

- determinare liberamente i fini e gli strumenti della sua azione politica interna grazie al suo:
  - **potere di prescrivere** (*power to prescribe*) provvedimenti amministrativi e legislativi;
  - **potere di imporre** (*power to enforce*), anche coattivamente, i propri provvedimenti;
- concorrere con gli altri soggetti dell'ordinamento internazionale alla determinazione di forme di organizzazione sociale tali da produrre posizioni soggettive (diritti e doveri) nell'ambito dei consociati.

4 Nell'ambito delle reti di calcolatori, la comunicazione tra due nodi non adiacenti deve attraversare tutti i nodi intermedi, percorrendo i rami relativi: ogni passaggio tra due nodi viene detto salto o *hop*.

5 Una VPN (*Virtual Private Network*) è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

6 In linea generale con la locuzione inglese *"data retention"* ci si riferisce al tempo di conservazione dei dati di *backup*, ossia il periodo utile in cui un *backup* è disponibile per il ripristino. Nell'ambito delle indagini informatiche, tale attività viene riferita specificatamente al periodo di conservazione dei dati di traffico telefonico e/o telematico (c.d. *file* di *log*) ai sensi art. 24 L.167/2017 e dell'art.132 D.Lgs. 196/2003 co. 1 e 3.

7 Le tecniche di NAT (*Network Address Translation*) vengono adottate dagli ISP per sopperire alle mancanze di IP (v.4) da attribuire ai propri clienti collegati alla rete Internet in un dato momento.

In alcune circostanze, tale soluzione si è rivelata una vera a propria tecnica di *antiforensics*, in quanto, a meno di conoscenza *ab origine* della c.d. *"porta di servizio"*, non consente l'identificazione univoca dell'utente o abbonato (art. 5 D.Lgs. 109/2008), costringendo così l'investigatore a lavorare su una pletora di utenze *«potenzialmente indiziarie»*.

8 *ex* artt. 14 D.Lgs. 70/2003 e 25 D.Lgs. 259/2003.

9 Il *"Proxy Registration Service"* consiste nel pagare una terza persona, generalmente una società, per inserire nel Whois le proprie informazioni personali.

10 Reg. (UE) n. 679/2016 e D. Lgs. n. 101/2018 che ha modificato il Codice Privacy al D.Lgs. n. 196/2003.

11 Il Whois è un database di pubblica consultazione che consente, in particolare, di visualizzare le informazioni del titolare di un dominio: cognome, nome, azienda (se applicabile), numero di telefono, indirizzo postale e di posta elettronica. Questo servizio storico del Web, la cui creazione risale al 1982, all'epoca permetteva di censire e identificare chiunque trasmettesse informazioni attraverso la rete Arpanet, antenata di Internet.

12 L'ICANN, quale ente di diritto americano e principale autorità di gestione della rete Internet e di attribuzione dei domini di primo livello (gTLD), esegue controlli regolarmente richiedendo annualmente, tramite il Registrar, la copia dei documenti che attestano l'identità del titolare ed ha il potere di domandare la sospensione del dominio in caso di dati mendaci.

13 Fortunatamente la maggior parte dei domini di primo livello (ccTLD) non sono soggetti a tale *"censura"*.

14 Il termine *sexting* è una parola composta, di origine anglosassone, derivato dalla fusione delle parole *sex* (sesso) e *texting* (inviare messaggi elettronici) e viene utilizzato per indicare l'invio di messaggi multimediali (testo, immagini e video) sessualmente espliciti, principalmente tramite i sistemi di *instant messaging* (es. WhatsApp e Telegram) o altri sistemi telematici.

15 Con la locuzione *"diritto all'oblio"* ci si riferisce ad un istituto di interpretazione giurisprudenziale, mai oggetto di un'apposita normativa,

gere" un dato (e la rispettiva informazione);
- una **"*certezza del diritto*"** subordinata:
  - alla sussistenza dei principi di reciprocità[16] e proporzionalità giuridica[17] tra Stati. Questo perché la maggior parte delle condotte antigiuridiche assunte in tale ambito operativo, corrispondono, da un punto di vista meramente materiale, alle medesime dei c.d. **"*reati transnazionali*"** *ex* art. 3 L. 146/2006[18];
  - alla diffusa presenza di *"vuoti legislativi"* dovuti alla differenze di velocità evolutiva tra la tecnologica ed il diritto (penale). Per tale motivo, gli operatori giuridici interni, per cercare di tenere il passo, sono costretti il più delle volte ad adottare un'**interpretazione funzionale** (scopo)[19] **ed evolutiva** (contesto attuale di riferimento)[20] delle norme.

2. I principali elementi costitutivi del *cyberspace*

Il processo di comprensione di un argomento consta nella quasi totalità di una fase di individuazione e definizione dei termini che ne costituiscono le fondamenta. È in tale logica che si inserisce questo paragrafo, volto a fornire un quadro normativo di riferimento utile a chi si accosti allo studio dell'ambiente complesso ed articolato del *cyberspace*.

a. Le fonti del diritto

Il Legislatore Italiano, spesso in adempimento di obblighi di cooperazione europea od internazionale, ha introdotto nell'ordinamento diverse disposizioni aventi come oggetto la tutela dei *"Sistemi Informatici o Telematici"*, ovvero il contrasto di condotte illecite realizzate per il loro tramite, come ad esempio:
- L.197/1991: Norme per prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio;
- L.547/1993: Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
- L.269/1998: Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, anche condotti per via telematica;
- L.248/2000: Modifiche alla legge 633/1941, in tema di diritto d'autore;
- D.L.vo 196/2003: Codice in materia di protezione di dati personali, così come modificato dalla Legge n. 45/2004 e seguenti;
- D.L.vo 82/2005: Codice dell'amministrazione digitale, quali norme in materia di documentazione informatica e di firma elettronica e digitale;
- L.38/2006: Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet;
- D.L.vo 231/2007 – art.55: Utilizzo indebito di titoli di pagamento, così come modificato dall'art. 4 del D. Lgs. 21/2018, che ha introdotto l'art. 493 *ter* c.p.;
- L.48/2008: Ratifica ed adattamento della Convenzione sul Cybercrime del Consiglio d'Europa (CETS N.185/2001);
- L.12/2012: Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica;

che costituisce il rovescio della medaglia del diritto all'informazione. Questi trae fondamento nel *diritto alla riservatezza* (artt. 2 e 21 Cost.) invocato da parte del soggetto cui i dati si riferiscono (Cass. 3679/1998), il quale richiede che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultano oramai dimenticate o ignote alla generalità dei consociati. Il diritto all'oblio tutela di fatto l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni potenzialmente lesive in ragione della perdita di attualità delle stesse, per cui il loro trattamento non risulta più giustificato e, anzi, è suscettibile di danneggiare il soggetto nella propria identità personale o morale nel momento storico attuale (Cass. 7769/1985). Emerge, allora, la necessità di garantire al soggetto la contestualizzazione e l'aggiornamento della notizia di cronaca che lo riguarda, e cioè il collegamento della notizia ad altre informazioni successivamente pubblicate riguardanti l'evoluzione della vicenda, che possano completare o mutare il quadro che si ricava dalla notizia originaria, a maggior ragione se si tratta di fatti oggetto di vicende giudiziarie.

16 Principio di reciprocità, mutuato dall'ambito privatistico, poiché richiede un rapporto sinallagmatico tra le parti, in modo tale da garantire un rapporto paritario (o simmetrico) delle relazioni giuridiche tra Stati. Si pensi, ad esempio, ad una richiesta di mutua assistenza giudiziaria da parte dell'Italia nei confronti degli USA in materia di diffamazione, così come stabilito dal Trattato del 2006. Negli Stati Uniti, la diffamazione non è un reato; anzi, spesso le affermazioni contenute nei profili *social* ritenute lesive della reputazione altrui sono protette dal diritto alla libertà di espressione, ai sensi del Primo Emendamento della Costituzione statunitense. La libertà di espressione negli Stati Uniti gode di un regime privilegiato e per questo motivo è considerato un *"interesse pubblico essenziale dello Stato"* ai sensi dell'Articolo 5 (*"Motivi Ostativi all'Esecuzione"*) del predetto Trattato.

17 Principio di proporzionalità, mutuato dall'ambito pubblicistico del potere internazionale, poiché idoneo a disciplinare i rapporti giuridici in cui vi è una parte che gode di supremazia (asimmetria), rispetto all'altra che si trova in una posizione di soggezione giuridica. La supremazia viene valutata in termini di poteri concessi da un ordinamento ad un organo interno dello Stato nell'esercizio (decentrato) delle sue funzioni di natura giuridico-amministrativa. Un esempio in merito è il bilanciamento fra i diritti individuali ed esigenze collettive nella tutela dei diritti dell'uomo.

18 La L. 146/2006 ha recepito solo in parte la Convenzione delle Nazioni Unite sottoscritta a Palermo il 12-15 dicembre 2000, ma ha definito la nozione di *"reato transnazionale"*, quale condotta punita con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato (art. 3 L. 146/2006), nonché:

a. sia commesso in più di uno Stato;
b. ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
c. ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
d. ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Nel caso si configuri un reato transnazionale è prevista sia una speciale aggravante (art. 4 L. 146/2006, così come modificato dal D.Lgs 21/2018 che ha introdotto l'art. 61 *bis* c.p.), che l'esecuzione di operazioni sotto copertura con ritardata notifica (art. 9 L.146/2006).

19 L'interpretazione funzionale di una norma giuridica è basata sulla valutazione dello scopo per la cui realizzazione il trattato/accordo è stato concluso.

20 L'interpretazione dinamica (o evolutiva) di una norma giuridica ritiene che il significato del dispositivo deve avvenire alla luce dei mutamenti dei costumi sociali presenti al momento dell'interpretazione del trattato/accordo.

- L.172/2012: Ratifica della Convenzione di Lanzarote per la protezione dei minori contro lo sfruttamento e l'abuso sessuale;
- L.119/2013: Aggravante specifica per la condotta di atti persecutori realizzata per il tramite di sistemi informatici o telematici;
- L.43/2015: Ratifica della Risoluzione n. 2178/2014 del Consiglio di Sicurezza dell'ONU;
- Regolamento UE 2016/679 : relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;
- D.Lgs. 108/2017: Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (17G00120);
- D.Lgs. 65/2018: Attuazione della Direttiva (UE) 2016/1148, c.d. Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi
- D.Lgs. 18 maggio 2018 n. 51 (entrato in vigore l'8 giugno 2018) : attuazione della direttiva (UE) 2016/680, quale relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Tra quelle elencate, oltre alla L.547/1993, la quale ha introdotto nel nostro ordinamento le prime norme di diritto sostanziale, sono di sicuro interesse le seguenti leggi che hanno fornito un'enorme propulsione alle attività investigative nel *cyberspace*:

- L. n. 48/2008, quale ratifica della Convenzione sul *Cybercrime* del Consiglio d'Europa (CETS N.185/2001), con la quale sono stati modificati numerosi mezzi di ricerca della prova (es. artt. 247 e 352 c.p.p. e ecc.), consentendo di eseguire attività di ricerca ed individuazione di dati in uno o più domicili informatici (Corte di Cassazione – Sez. VI Sent. n. 3067 del 14/12/1999; Sez. V Sent. n. 31135 del 6/7/2007[21] e Corte di Cassazione – Sez. V, Sent. n. 42021 del 26/10/2012[22]), sia locali che remoti[23], in cui i sistemi informatici e telematici costituiscono l'elemento materiale di questo *"nuovo"* scenario operativo;
- L. n. 43/2015, quale recepimento della Risoluzione n. 2178/2014 del Consiglio di Sicurezza dell'ONU, con la con la quale è stato introdotto un nuovo mezzo di prova denominato *"Acquisizione di documenti e dati informatici"* (art. 234-*bis* c.p.p.), il cui dettato normativo ricalca *de facto* l'art. 32 della Convenzione di cui al punto precedente. Tale norma fornisce piena ammissibilità dibattimentale ai dati informatici acquisiti da *"fonti aperte"*[24], ancorché presenti in territorio estero, ovvero forniti, senza alcuna forma di costrizione, da parte del *"legittimo titolare"* (o *Lawful Authority* - cfr. § par. 3.b) mediante una c.d. procedura di *"voluntary* o *emergency disclosure"*. La procedura in parola consente di fatto di bypassare le lungaggini amministrative derivanti dall'attivazione di un canale rogatoriale, le quali mal si addicono ad uno scenario operativo che, oltre a presentare le medesime peculiarità dei c.d. *"reati transnazionali"* (art. 3 L. 146/2006), è ulteriormente complicato dalla dinamicità e dalla volatilità del c.d. *"cyberspace"* (o ciberspazio).

Oltre ai suddetti aspetti di ordine procedurale e sostanziale, il Legislatore europeo e quello italiano poi, hanno regolamentato anche il trattamento dei dati personali da parte delle autorità competenti (es. AG, PG, PS ecc.) a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché salvaguardia e prevenzione di minacce alla sicurezza pubblica, quale combinato disposto del Regolamento UE 2016/679 e del D.Lgs. n. 51/2018 emanato in attuazione della direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Il trattamento dovrà avvenire nel rispetto dei seguenti principi:

- liceità e correttezza, ossia i dati raccolti per finalità sopra descritte non possono essere trattati per finalità diverse, salvo i casi previsti dal diritto dell'UE o dalla legge;
- adeguatezza, pertinenza e non eccedenza;
- esattezza e, se necessario, aggiornamento, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti;
- conservazione per il tempo necessario al conseguimento delle finalità per le quali sono trattati;
- garanzia di adozione di adeguate misure di sicurezza (tecniche e organizzative) e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

21 Corte di Cassazione (Sez. VI Sent. n. 3067 del 14/12/1999; Sez. V Sent. n. 31135 del 6/7/2007) «… *deve ritenersi "domicilio informatico", … quello spazio ideale (ma anche fisico in cui sono contenuti i* ***dati informatici****) di pertinenza della persona, cui si estende la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 15 Cost.)...».*

22 Corte di Cassazione (Sez. V, Sent. n. 42021 del 26/10/2012 «… *l'art. 615-ter c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "jus excludendi alios"*» (facoltà di escludere terzi non graditi).

23 In generale, in base all'art. 6 c.p. è prevista la punibilità per chiunque commetta un reato nel territorio dello Stato, anche se la condotta (azione od omissione) si sia tenuta solo in parte. A corroborare tale ipotesi è intervenuta la SC con le seguenti sentenze in materia di potestà punitiva dello Stato italiano in materia di condotte antigiuridiche commesse tramite il *cyberspace*:

- Corte di Cassazione (Sez. V Sent. n. 4741 del 27/12/2000) «… *La c.d. "teoria della ubiquità", dunque, consente al giudice italiano di conoscere del fatto-reato, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto in quello in cui su di esso si sia verificato l'evento. Pertanto, nel caso di un iter criminis iniziato all'estero e conclusosi (con l'evento) nel nostro paese, sussiste la potestà punitiva dello Stato italiano...»*
- Corte di Cassazione (Sez. IV Sent. n. 40903 del 28/06/2016) «… *la detenzione dei file all'interno di un singolo account protetto da password (come all'interno del proprio spazio cloud) è dell'utente che dispone di quella password. La detenzione consiste infatti nell'avere la disponibilità di una cosa, ossia nell'avere la possibilità di utilizzarla tutte le volte che si desideri, pur nella consapevolezza che essa appartiene ad altri, ai quali comunque si deve render conto (animus detinendi). Ebbene, tale potere … lo esercita soltanto chi è in possesso della password per accedere all'account ...»*

24 Fonte aperta (*open source*). Con tale locuzione si intende l'insieme dei *"dati pubblici"* ed *"aperti al pubblico"* consultabili da chiunque, come ad esempio quotidiani, periodici, elenchi telefonici, servizi Internet. In quest'ultimo caso, si parlerà di *"dati pubblici"* quando questi sono conoscibili a chiunque ed accessibili senza restrizioni non riconducibili a esplicite norme di legge, così come sancito dal Codice dell'Amministrazione Digitale (art. 1 lett. n ed o del D.Lgs. n. 82/2005 - CAD), mentre la nozione del *"dato aperto al pubblico"* è un concetto di interpretazione giurisprudenziale derivato dalla sentenza 11 luglio 2014 (dep. 12/09/2014) n. 37596 della Corte di Cassazione, la quale ha assimilato una pagina pubblica (visibile a chiunque sia registrato) di un *social network*, nella fattispecie Facebook, come un luogo aperto al pubblico.

Le categorie di soggetti interessati dal provvedimento sono:
- gli indagati e gli imputati (anche se in un procedimento connesso o collegato);
- i condannati con sentenza definitiva;
- le persone offese dal reato;
- le parti civili;
- le persone informate sui fatti e testimoni.

Nell'ambito di questo intervento legislativo risulta di particolare interesse il fatto che:
- (art. 8) l'interessato ha il diritto di non essere sottoposto a una **decisione basata unicamente**[25] **sul trattamento automatizzato** (es. tramite Intelligenza Artificiale). Tale disposizione non si applica nel caso in cui la procedura sia autorizzata dall'Unione Europea o Stato membro; ci sia il consenso dell'interessato. Ad ogni modo, possiamo ribadire che l'attuale sistema giudiziario penalistico impedisce una decisione determinata in modo esclusivo da una tale fattispecie di algoritmo alla luce degli evidenti limiti normativi (soprattutto costituzionali) e ed evidenti diritti e libertà fondamentali dell'interessato (*in primis* il diritto ad un giusto processo ed al contraddittorio) che verrebbero compromessi con l'utilizzo di tale soluzione;
- (art. 25) il titolare del trattamento e il responsabile del trattamento devono adottare **misure tecniche e organizzative** per garantire un livello di sicurezza adeguato rispetto al rischio di violazioni dei diritti e delle libertà delle persone fisiche (ex art. 32 G.D.P.R. - D.Lgs. 101/2018). A tal proposito si pensi:
  - alla pseudonimizzazione dei dati in modo tale che i dati stessi non potranno più essere attribuiti direttamente ed automaticamente ad un interessato specifico;
  - alla capacità di assicurare la continua riservatezza[26] (cifratura), integrità[27] (*hashing*), disponibilità (ACL - Liste di controllo accessi) e resilienza dei sistemi e dei servizi che trattano i dati;
  - all'adozione di piani di *incident response* (risposta agli incidenti informatici) finalizzati al giusto bilanciamento tra le esigenze di *disaster recovery*, ossia la capacità di ripristinare tempestivamente la disponibilità[28] dei dati in caso di incidente fisico o tecnico, e di giustizia (*digital forensics*), ossia l'insieme delle attività finalizzate all'acquisizione, preservazione ed analisi dei dati informatici presenti sulla scena del crimine;
  - alla capacità di *auditing* interno ed esterno, ossia una procedura per provare, verificare e valutare regolarmente, anche da parte di soggetti terzi, le misure tecniche e organizzative al fine di garantire l'efficacia ed efficienza delle stesse.

b. La figura del *"legittimo titolare"*

La figura del *"legittimo titolare"*, ergo della *"lawful authority"* (*ex* art. 32 della CETS N.185/2001), che concettualmente andrebbe tradotto dall'inglese come *"persona legalmente autorizzata"*, è una delle nozioni che più si presta a dubbia interpretazione nell'ambito delle attività connesse al contrasto della criminalità informatica.
È da escludersi a priori che tale soggetto possa coincidere con la figura dell'indagato, per il quale sono previste altre e specifiche garanzie e mezzi di ricerca della prova (es. *"res petita" ex* art. 248 c.p.p.). Ciò premesso, è facile dedurre che tale persona (fisica o giuridica) va individuata tra soggetti terzi (es. persona informata sui fatti, *provider* ecc.), la quale, da un punto di vista del diritto in generale, non può essere assimilato né alla figura del *"titolare del trattamento"*, quale nozione ereditata dal Regolamento (UE) 2016/679 (*ex* art. 4 par. 1 let. 7), né a quella del *"generatore"* o *"detentore"* (di fatto) del dato informatico.
A titolo di esempio si consideri il seguente scenario: Mario Rossi produce una fotografia, che viene inviata via WhatsApp a Giulia Bianchi, che a sua volta la carica sul suo *cloud storage* DropBox. In tale contesto operativo, nascono spontanee le seguenti domande volte a predire l'ammissibilità della fonte di prova digitale:
- chi è il legittimo titolare per la consegna del dato presente nel domicilio informatico di Giulia Rossi?
- chi ha prodotto (Mario Rossi), chi gestisce (Giulia Bianchi) o chi lo detiene (DropBox, che di fatto è una società che non ha propri *server* fisici, ma usufruisce del servizio *cloud platform as a service* di Amazon)?

Alla luce di questo vuoto legislativo, caratterizzato dalla mancata definizione formale di tale figura, l'esperienza operativa maturata in questi ultimi anni converge nell'individuazione del *"legittimo titolare"*, in quel soggetto che esercita un'azione di *"possesso"* tale da garantirgli un livello di autonomia che consente di accedere in modo autonomo al dato informatico, anche al di fuori della diretta vigilanza della persona che abbia sul dato un potere giuridico maggiore (es. titolare dell'*account*). Ovviamente tale peculiarità non dovrà essere solo *de facto*, ma anche *de jure*, ossia desunta dai termini del contratto sottoscritto con un dato utente.

c. La nozione di reato informatico

In virtù dei numerosi ordinamenti giuridici che possono essere coinvolti in una condotta antigiuridica eseguita in danno o per mezzo della rete Internet, attualmente non esiste una definizione universalmente riconosciuta di *cybercrime* (o diversamente detto *computer crime*). Una delle più autorevoli è stata fornita dall'Unione Europea[29], secondo la quale deve considerarsi *cybercrime*:

«any criminal acts associated with computers, networks, ICT and online activity».

All'occhio attento del lettore penalista, tale definizione non può ritenersi esaustiva, in quanto scevra di una componente fonda-

25 L'inciso *"unicamente"* potrebbe suggerire che il giudice possa avvalersi (appunto non esclusivamente) dell'algoritmo per esprimere un giudizio.

26 Riservatezza: requisito di sicurezza che esprime la protezione da divulgazione non autorizzato delle informazioni. In altri termini, i dati devono essere accessibili esclusivamente a coloro che ne sono i legittimi fruitori.

27 Integrità: requisito di sicurezza che esprime la protezione da modifiche non autorizzate ai dati da parte di chi non ne ha diritto.

28 Disponibilità: requisito di sicurezza che esprime la protezione dall'impossibilità di utilizzo di un dato da parte di chi è legittimato a farlo nei termini stabiliti dal servizio.

29 https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf

mentale di quello che con il termine inglese *"crime"* dovremmo tradurre come *"reato"*[30], ossia l'elemento soggettivo del reato[31], nonché la possibilità che si possano presentare anche delle c.d. *"cause di giustificazione"*[32] (teoria tripartita del reato), come ad esempio l'adempimento di un dovere (*ex* art. 52 c.p.).
Alla luce di tali considerazioni e dallo studio delle attuali pene comminate per le condotte in parola, oltre al *"fatto tipico"* presente nella prefata definizione, possiamo definire quindi un **reato informatico** come:

«un delitto commissivo punibile a titolo di dolo in danno o per mezzo della tecnologia dell'informazione (sistema informatico o telematico, dati, informazioni, programmi ...)»[33].

Da un punto di vista più operativo, enti autorevoli come Interpol[34] e EuroPol - EC3[35] distinguono nello specifico:
- reati commessi in danno dei sistemi informatici e telematici, detti anche *advanced cybercrime* (oppure *high-tech crime* o *cyber-dependent crime*), come ad esempio condotte commesse mediante tecniche di *hacking* (D-DOS, Botnet, Zombi, ...), *crimeware* (Virus, Worm, Trojan, ecc.), *spamming* ecc.;
- reati commessi per mezzo dei sistemi informatici e telematici, detti anche *cyber-enabled crime*, come ad esempio reati in materia di pornografia minorile, reati finanziari, terrorismo, atti persecutori, ecc.

Nella figura sottostante viene fornita una sintetica ma significativa comparazione dei reati commessi nel mondo reale e quello virtuale, evidenziando di volta in volta le eventuali fattispecie autonome. ©

Figura 1 - Comparazione tra reati nel mondo reale e quello virtuale

30 Reato è un fatto umano, commissivo o omissivo, previsto dalla legge (principio di legalità) in modo preciso (principio di tassatività), ed attribuibile ad un soggetto (principio della personalità della responsabilità penale) sia causalmente (principio di materialità) che psicologicamente (principio di soggettività), offensivo di un bene giuridico costituzionalmente rilevante (principio di offensività) e sanzionato da una norma preesistente al momento della commissione del fatto (principio di irretroattività), che preveda una pena proporzionata alla gravità del fatto e tesa alla rieducazione del condannato (principio del finalismo rieducativo della pena).

31 Gli elementi soggettivi del reato (dolo, colpa e preterintenzione) presuppongono la consapevolezza e l'imputabilità del soggetto attivo (autore) del reato.

32 Le Cause di giustificazione (o scriminanti), dette anche cause oggettive di esclusione del reato: esse incidono sull'elemento oggettivo del reato (Condotta, Evento e Nesso di Casualità) e ne escludono l'antigiuridicità e la dannosità sociale, ovvero vanno esenti da pena, in quanto, per il principio di non contrapposizione, non si può imporre o vietare uno stesso comportamento all'interno di una norma.

33 Mappatura della ISO 27037:2012 al Cloud Computing – pag. 20 – Tesi Master di Primo Livello in Digital Forensics di Giuseppe Specchio presso l'Università di Modena e Reggio Emilia.

34 https://www.interpol.int/content/download/5267/file/Cybercrime.pdf

35 https://www.europol.europa.eu/iocta/2018 e https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime