

INTRODUZIONE

La progressiva digitalizzazione delle attività individuali, economiche e amministrative ha trasferito una parte crescente delle relazioni sociali all'interno dei sistemi informatici e delle reti telematiche. Il sistema informatico non costituisce più soltanto uno strumento di elaborazione o conservazione delle informazioni, ma rappresenta uno spazio nel quale si svolgono attività personali, professionali e istituzionali, dando vita a un vero e proprio «habitat cibernetico»¹.

Tale trasformazione ha interessato in modo particolarmente significativo la Pubblica Amministrazione. Il progressivo superamento del modello cartaceo e la diffusione di sistemi informativi, banche dati e documenti digitali hanno modificato le modalità di formazione, consultazione, conservazione e trasmissione delle informazioni². Alla crescente disponibilità tecnologica si è tuttavia accompagnata l'emersione di nuove forme di aggressione agli interessi giuridicamente protetti. Un passaggio fondamentale è rappresentato dalla legge 23 dicembre 1993, n. 547, che ha introdotto specifiche fattispecie di criminalità informatica, tra le quali assume particolare rilievo l'art. 615-ter c.p., relativo all'accesso abusivo a un sistema informatico o telematico³.

La stessa utilizzazione del verbo «introdursi» trasferisce nella dimensione immateriale del sistema informatico una categoria originariamente riferita allo spazio fisico. Da tale impostazione si è sviluppata la nozione di domicilio informatico, mentre l'evoluzione tecnologica ha progressivamente ampliato il problema del bene giuridico tutelato: non soltanto riservatezza, ma anche

¹ M. LAMANUZZI, *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma*, in *Archivio Penale*, 2022, n. 1, p. 3, sul concetto di «habitat cibernetico»

² D.lgs. 12 febbraio 1993, n. 39; d.lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale.

³ L. 23 dicembre 1993, n. 547; sull'evoluzione della tutela penale in materia di criminalità informatica, v. L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova, 2004, pp. 21 ss.

esclusività e sicurezza dell'accesso, controllo del sistema, confidenzialità, integrità e disponibilità dei dati⁴.

A questo processo si affianca oggi un articolato quadro sovranazionale. La Convenzione di Budapest del 2001, ratificata dall'Italia con la legge n. 48 del 2008, ha rafforzato la tutela penale e la cooperazione internazionale in materia di criminalità informatica. Nel più recente quadro europeo, il GDPR disciplina la protezione delle persone fisiche rispetto al trattamento dei dati personali, mentre l'AI Act interviene sullo sviluppo e sull'utilizzazione dei sistemi di intelligenza artificiale, secondo un modello fondato sul rischio, sulla tracciabilità e sulla supervisione umana. L'AI Act segna un significativo mutamento di prospettiva, spostando l'attenzione dalla sola disciplina del dato al funzionamento dei sistemi di intelligenza artificiale e ai processi decisionali automatizzati, attraverso un modello fondato sul risk management, sulla documentazione, sulla tracciabilità delle operazioni e sulla supervisione umana⁵.

Sul diverso versante dell'acquisizione della prova digitale si colloca il sistema europeo dell'e-Evidence, fondato sul regolamento (UE) 2023/1543 e sulla direttiva (UE) 2023/1544, relativo alla produzione e alla conservazione delle prove elettroniche nei procedimenti penali.

Il problema dell'accesso abusivo presenta quindi una duplice dimensione. La prima riguarda il soggetto estraneo che accede al sistema senza titolo; la seconda, più complessa, riguarda chi disponga legittimamente delle credenziali, ma possa oltrepassare i limiti dell'autorizzazione. La questione assume particolare rilievo per il pubblico ufficiale, rispetto al quale la possibilità materiale di consultare un dato non coincide necessariamente con la legittimazione giuridica a farlo. La dottrina ha infatti evidenziato la necessità di distinguere l'abuso della

⁴ M. LAMANUZZI, *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma*, in *Archivio Penale*, 2022, n. 1.

⁵ Reg. (UE) 2016/679; Reg. (UE) 2024/1689; interventi del convegno CyberShield II – Cybersecurity for AI and AI for Cybersecurity.

funzione dall'abusività dell'accesso, valorizzando i profili-limiti di autorizzazione⁶.

Una nuova zona problematica può inoltre derivare dall'impiego di sistemi di intelligenza artificiale capaci di interagire con banche dati e sistemi informatici. Qualora l'operazione sia materialmente eseguita da un sistema automatizzato attraverso le credenziali o nell'ambito dei poteri attribuiti all'operatore umano, occorre stabilire entro quale perimetro si estenda l'autorizzazione e a chi sia imputabile l'eventuale superamento dei relativi limiti.

La questione coinvolge quindi, oltre al profilo oggettivo dell'accesso, anche quello dell'imputazione della condotta e dell'elemento soggettivo.

La ricerca si propone pertanto di verificare quando il superamento dei limiti dell'accesso rimanga sul piano dell'irregolarità o dell'illegittimità e quando, invece, raggiunga la soglia della rilevanza penale, con particolare attenzione all'accesso del soggetto autorizzato, del pubblico ufficiale e alle attività investigative, di controllo e ispettive. Il filo conduttore dell'indagine può essere sintetizzato nella considerazione secondo cui la possibilità tecnica di accedere al dato non coincide necessariamente con la legittimazione giuridica ad acquisirlo o utilizzarlo.

⁶ R. FLOR, *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere"*, in *Diritto penale e processo*, 2018, n. 4, pp. 506-515

CAPITOLO PRIMO

Tecnologie digitali e tutela dei beni giuridici

1.1 La trasformazione digitale dell'attività investigativa e ispettiva

La digitalizzazione non rappresenta soltanto un progresso tecnologico, bensì una trasformazione strutturale della società contemporanea, nella quale dati, informazioni e comunicazioni costituiscono il principale fattore di produzione economica e di esercizio delle libertà individuali. La progressiva informatizzazione delle attività pubbliche e private non ha infatti comportato un semplice mutamento degli strumenti utilizzati per comunicare, archiviare o elaborare informazioni, ma ha inciso sulla struttura stessa delle relazioni sociali, economiche e istituzionali. L'informazione digitale è divenuta un elemento essenziale dell'organizzazione della società divenuta digitale anch'essa, assumendo un valore autonomo quale bene economico, strumento di esercizio dei diritti e presupposto dell'attività amministrativa e giurisdizionale.

La trasformazione digitale ha investito in maniera trasversale tutti i settori dell'ordinamento. Le pubbliche amministrazioni hanno progressivamente sostituito gli archivi cartacei con banche dati informatizzate, sviluppato piattaforme interoperabili⁷ e introdotto procedure interamente telematiche per l'erogazione dei servizi e lo svolgimento delle attività di controllo. Parallelamente, anche il settore privato ha visto una crescente dipendenza dai sistemi informatici per la gestione dei processi produttivi, delle comunicazioni, dei dati aziendali e

⁷ L'interoperabilità nella pubblica amministrazione è la capacità dei sistemi informatici degli enti pubblici di scambiarsi dati in modo sicuro e automatico. I suoi elementi chiave sono la Piattaforma Digitale Nazionale Dati (PDND) gestita dalla Presidenza del Consiglio, il principio *once-only* ovvero evitare di chiedere ai cittadini e alle imprese dati che la pubblica amministrazione possiede già, e le API standard, acronimo di *Application Programming Interface* (interfaccia di programmazione delle applicazioni). In informatica, è un insieme di regole e strumenti che permette a diversi programmi o software di comunicare tra loro e scambiarsi dati in modo semplice e sicuro.

delle informazioni strategiche. In tale contesto, il sistema informatico non rappresenta più un semplice strumento operativo, ma costituisce il luogo nel quale si svolge una parte significativa delle relazioni giuridiche.

L'evoluzione tecnologica ha inevitabilmente modificato anche le modalità di esercizio delle funzioni investigative e ispettive. È cambiato ciò che la Polizia Giudiziaria deve cercare. Se tradizionalmente l'accertamento dei fatti si fondava sull'acquisizione di documenti cartacei, sull'ispezione di luoghi fisici e sulla raccolta di testimonianze, oggi una parte rilevante dell'attività conoscitiva si sviluppa attraverso l'analisi di dati digitali, registri elettronici, metadati, sistemi di autenticazione, log di accesso e banche dati interconnesse. La prova tende così a smaterializzarsi, assumendo una dimensione prevalentemente digitale. Nell'attuale ecosistema tecnologico le informazioni non coincidono più con il supporto materiale che le contiene, ma sono frequentemente conservate in infrastrutture cloud, distribuite tra molteplici data center e continuamente replicate per garantirne disponibilità e resilienza. Il dato perde pertanto il tradizionale collegamento con un luogo fisico determinato, assumendo una natura potenzialmente ubiqua. Tale evoluzione modifica profondamente anche l'attività investigativa e ispettiva, chiamata non più a ricercare il documento materiale, bensì a ricostruire un patrimonio informativo dinamico, distribuito e spesso privo di una localizzazione territoriale univoca. La crescente delocalizzazione delle prove digitali ha reso necessario l'adozione di strumenti di cooperazione giudiziaria sovranazionale, oggi significativamente rafforzati dal cosiddetto *e-Evidence Package*⁸.

Particolarmente significativa risulta la trasformazione dell'attività ispettiva svolta dalle pubbliche amministrazioni. L'evoluzione normativa in materia di amministrazione digitale ha progressivamente favorito l'integrazione tra archivi

⁸ Sul rafforzamento degli strumenti di cooperazione giudiziaria in materia di prove elettroniche, v. la Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23 novembre 2001), il Secondo Protocollo Addizionale del 12 maggio 2022 e il cosiddetto e-Evidence Package, composto dal Regolamento (UE) 2023/1543 e dalla Direttiva (UE) 2023/1544, entrambi del Parlamento europeo e del Consiglio del 12 luglio 2023.

pubblici, consentendo agli organi di controllo di accedere, nei limiti previsti dalla legge, a una pluralità di sistemi informativi e di banche dati istituzionali. L'attività ispettiva non si esaurisce più nell'esame della documentazione esibita dal soggetto controllato, ma si fonda sempre più frequentemente sull'interrogazione di sistemi informatici, sulla verifica incrociata delle informazioni e sull'utilizzo di strumenti digitali capaci di ricostruire in tempo reale dati, operazioni e flussi documentali.

Tale evoluzione presenta indubbi vantaggi in termini di efficienza, rapidità e completezza dell'azione amministrativa. L'interoperabilità tra banche dati, l'automazione di numerosi procedimenti e l'impiego di strumenti di analisi digitale consentono infatti di migliorare la capacità di prevenzione, controllo e accertamento delle violazioni. Allo stesso tempo, tuttavia, l'ampliamento dei poteri conoscitivi attribuiti ai soggetti pubblici impone una costante attenzione alla tutela dei diritti fondamentali, affinché l'innovazione tecnologica non determini un indebito sacrificio della riservatezza, della libertà personale e dell'autodeterminazione informativa.

Tuttavia, la crescente centralità della prova informatica impone di ripensare non soltanto le garanzie difensive, ma anche i criteri di attendibilità dell'accertamento tecnico-scientifico. La natura facilmente modificabile del dato digitale richiede infatti il rigoroso rispetto delle metodologie di acquisizione e conservazione dell'evidenza informatica per garantirne la genuinità, attribuendo al giudice un ruolo essenziale nella verifica della correttezza scientifica delle operazioni compiute e della conseguente affidabilità del risultato probatorio⁹.

La digitalizzazione modifica, inoltre, il contenuto stesso dei beni suscettibili di protezione giuridica. Nella tradizionale concezione del diritto penale, la tutela era prevalentemente rivolta a beni materiali o comunque riferibili a una dimensione fisica della persona e del patrimonio. L'affermarsi delle tecnologie

⁹ Cfr. A. SANNA, *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, in *DisCrimen*, 4 maggio 2022, spec. §§ 2-3: “La genuinità della prova digitale è compromessa se gli investigatori non osservano le migliori metodologie scientifiche (...). Il rimedio contro questi rischi consiste nel ruolo di guardiano esercitato dal giudice contro la cattiva scienza e i cattivi scienziati.”

informatiche ha invece determinato la progressiva emersione di nuovi interessi meritevoli di protezione, quali l'integrità dei sistemi informatici, la sicurezza delle infrastrutture digitali, la disponibilità dei dati, la riservatezza delle comunicazioni elettroniche e il controllo sull'accesso alle informazioni custodite negli archivi digitali.

Come evidenziato dalla più autorevole dottrina, il fenomeno non può essere interpretato come un semplice ampliamento dell'ambito applicativo delle categorie tradizionali. La trasformazione digitale ha infatti inciso sulla stessa nozione di bene giuridico, imponendo una riflessione sull'idoneità delle categorie penalistiche elaborate in un contesto analogico a descrivere realtà profondamente mutate. Il sistema informatico diviene così non soltanto il mezzo attraverso cui possono essere commessi nuovi reati, ma anche l'oggetto diretto della tutela penale, quale ambiente nel quale si svolgono attività economiche, amministrative e personali di fondamentale rilievo.

L'adeguamento dell'ordinamento a tale evoluzione è avvenuto progressivamente. La legge 23 dicembre 1993, n. 547 ha rappresentato il primo intervento organico volto a disciplinare la criminalità informatica, introducendo nel Codice Penale nuove fattispecie incriminatrici finalizzate a garantire la tutela dei sistemi informatici e telematici.

Successivamente, la Convenzione di Budapest del 2001 ha contribuito a delineare un quadro internazionale uniforme nella repressione del cybercrime, mentre il legislatore europeo ha ulteriormente sviluppato la disciplina attraverso strumenti quali il Regolamento (UE) 2016/679 (GDPR), la Direttiva (UE) 2022/2555 (NIS2) e il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (AI Act)¹⁰. Sebbene tali fonti perseguano finalità differenti, esse condividono

¹⁰ Il Regolamento (UE) 2016/679 (GDPR) disciplina la protezione dei dati personali e la tutela dei diritti degli interessati; la Direttiva (UE) 2022/2555 (NIS2) rafforza gli obblighi di cybersicurezza e resilienza delle reti e dei sistemi informativi degli operatori pubblici e privati; il Regolamento (UE) 2024/1689 (AI Act) introduce il primo quadro normativo europeo per lo sviluppo e l'impiego dei sistemi di intelligenza artificiale, fondato su un approccio basato sul rischio.

l'obiettivo di rafforzare la tutela dello spazio digitale quale ambiente nel quale si esercitano diritti fondamentali e interessi collettivi di crescente rilevanza che devono trovare l'equilibrio con l'efficacia investigativa che deve rispettare i principi di legalità, necessità e proporzionalità della sfera digitale della persona come affermato dalla CEDU e dalla Corte EDU¹¹.

La trasformazione digitale non ha inciso soltanto sugli strumenti attraverso i quali vengono svolte le attività investigative e ispettive, ma ha determinato una profonda evoluzione dei beni giuridici meritevoli di tutela penale. La centralità assunta dai sistemi informatici, dalle banche dati e dalle informazioni digitali impone di verificare se categorie tradizionali, quali la riservatezza e il domicilio, siano ancora sufficienti a descrivere il contenuto della tutela predisposta dall'ordinamento oppure se l'evoluzione tecnologica abbia determinato l'emersione di nuovi interessi giuridicamente rilevanti. Tale problematica costituisce il naturale punto di partenza dell'analisi del bene giuridico tutelato dall'art. 615-ter c.p., cui è dedicato il paragrafo che segue.

1.2 Il bene giuridico tutelato nell'era digitale: dalla riservatezza al controllo del sistema informatico

L'individuazione del bene giuridico tutelato costituisce il presupposto fondamentale per la corretta interpretazione della norma penale. Il bene giuridico non svolge infatti una funzione meramente descrittiva dell'interesse protetto dalla fattispecie incriminatrice, ma rappresenta il criterio attraverso il quale delimitarne l'ambito applicativo, verificarne la concreta offensività e ricostruire la *ratio* dell'intervento legislativo. Nei reati informatici tale operazione assume una

¹¹ L'art. 8 della *Convenzione europea dei diritti dell'uomo (trattato internazionale Roma 4 novembre 1950)* riconosce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, ricomprendendovi dati personali, comunicazioni elettroniche, attività svolte online, informazioni contenute nei dispositivi digitali.

La Corte europea dei diritti dell'uomo ha esteso l'ambito applicativo dell'art. 8 alle nuove forme di comunicazione e inoltre affermato che ogni interferenza dell'autorità pubblica deve rispettare i principi di legalità, necessità e proporzionalità, principi che hanno influenzato profondamente anche il diritto processuale penale italiano.