diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Tutela dei diritti e mondi intrusivi digitali

Autore: Alessandro Biamonte
In: Diritto amministrativo

L'inconscio digitale tra cybersecurity e data protection.

Abstract: Le dinamiche pervasive della rete, segnate da un intrusivo sviluppo progressivo nella vita quotidiana, e l'interconnessione dei sistemi rendono improcastinabile, al di là delle previsioni normative più recenti (Regolamento GDPR n. 2016/679/EU, Regolamento sulla vita privata elettronica e Direttiva cd. NIS n. 2016/1148/EU), la realizzazione di un assetto effettivo di tutele che – al passo con l'evoluzione tecnologica – garantisca, al tempo stesso, la sicurezza strategica delle infrastrutture e la protezione dei dati individuali (Data Protection) da un incontrollato sistema (non statuale e ageografico) di tracciatura e profilazione – sospeso tra analisi statistica e acquisizione di dinamiche dell'inconscio – . In questo contesto, assume valenza dirimente la nozione di «sovranità digitale» come snodo della necessaria tutela statuale in ambito nazionale e internazionale.

La tutela dei diritti e l'inconscio digitale

Lo sviluppo pervasivo e, al tempo stesso, invasivo, in termini pandigitali, della rete nella vita quotidiana (si pensi solo all'internet of thinks, dove ogni oggetto – anche il più banale, come un frigorifero, un climatizzatore o un forno – finisce con il divenire elemento attivo della rete nella raccolta, condivisione e trasmissione delle informazioni) è ormai divenuto funzionale a un sistema di circolazione e conservazione di quegli elementi così acquisiti (addirittura suscettibile di valutazione in termini economici in proporzione alla loro aggregazione), contribuendo all'affermazione di un mondo intrusivo in cui i dati stessi (in primis i Big Data, ma anche le profilazioni e la tracciatura dei fruitori) diventano parte di un sistema di classificazione di conoscenze di dominio capace di intervenire nella psiche e condizionarla ad un livello pre-riflettente.

Questo incedere, progressivo e inesorabile, impone nuovi e più rafforzati metodi di prevenzione a tutela degli stessi e della libertà dell'individuo: ogni giorno, e nelle azioni più inconsapevoli, finiamo con l'autospogliarci di ogni filtro, consegnando le nostre vite nelle mani di recettori dei quali non sappiamo nulla, ma che analizzano, tracciano e profilano sino a delineare uno psicoprogramma individuale o collettivo dell'inconscio. Si immettono volontariamente – in modo diretto o indiretto – informazioni personali senza conoscere, spesso, chi le raccolga o le acquisisca nella catena finale finendo con il detenerle in modo pressoché definitivo e incontrollato. Ed è proprio l'incertezza sul controllo (e sui possibili rimedi o tutele esperibili) a minare gravemente la libertà.

Siamo cresciuti nel mito della crescita esponenziale della comunicazione interconnessa come esperienza somma di libertà, senza renderci conto che, in mancanza del consolidamento di un consapevole assetto di tutele, quell'autodenudamento volontario potrebbe essere strumentale (anzi, già lo è) a un potere subdolo, per così dire «intelligente» e dunque più deflagrante del potere repressivo, che non nega la libertà, ma la «sfrutta» in un sistema di autoesposizione (quasi un capitalismo del like), realizzando paradossalmente il programma per mezzo di un «autosfruttamento» dello stesso utilizzatore di sconosciute forme immateriali di produzione, fino a porre in crisi le categorie classiche del conflitto sociale fondate sulla evoluzione traumatica dei rapporti di produzione. Oggi questa nevrosi finisce con il coinvolgere l'individuo in sé, nella misura in cui la lotta interiore con se stessi (tra sfruttatore e sfruttato) si traduce in un patologico burnout indotto da una libertà che finisce con lo sfociare in (inconsapevole) costrizione. I big data rispondono a un sistema di lettura inconscia dei desideri e, se si considera il sistema ormai evoluto dei sistemi di profilatura e tracciatura individualizzata (con correlata archiviazione delle preferenze di ciascun soggetto) secondo un processo di intelligenza artificiale, si perviene a un sistema di lettura della psiche più veloce della volontà libera: di qui al totalitarismo digitale il passo è breve. Le emozioni sono regolate dal sistema limbico, che è anche la sede degli impulsi. Il loro sfruttamento per mezzo della archiviazione intelligente delle preferenze di ciascuno consente di accedere al loro controllo secondo un livello pre-riflettente, per il quale un sistema evoluto (secondo schemi algoritmici) è in grado di conoscere – anticipatamente e in modo esplicito – sia l'azione corporea istintiva sia l'effetto psichico. La detenzione di queste informazioni assume un valore giuridico assoluto, che non solo non può essere sottratto a tutela, ma non può essere destinato a un (comodo?) limbo normativo, fosse solo per l'imperativo che discende dall'obbligo di tutela dei diritti involabili immanente al nostro ordinamento costituzionale.

Ben più di ciò che aveva prefigurato Orwell, laddove il Grande Fratello agiva in un contesto di sorveglianza di carattere «disciplinare» (fondata cioè su prescrizioni e divieti in senso inibitorio) – per dirla con Jeremy Bentham[2] –, mentre il serpeggiante sistema di psicopotere sotteso allo status quo pandigitale, abbandonando i divieti, utilizza stimoli positivi e incoraggia l'incontrollata circolazione delle informazioni secondo lo schema aprospettico di un panottico digitale (e non più analogico, come in Bentham) che fornisce (e archivia in modo definitivo) una categorizzazione intelligente di «ciascuna» persona. Oggi nessuno si sente sorvegliato, o minacciato in modo esplicito, ed è questo stato a costituire l'essenza del problema da affrontare con efficaci strumenti giuridici.

Big data, profilazione e tracciatura danno accesso all'inconscio regno di azioni e inclinazioni. Ciò deve indurre a riflettere e ad agire in modo direttamente proporzionale all'evoluzione dei sistemi intelligenti complessi: non si tratta semplicemente di conoscenza astratta e aggregata dell'inconscio collettivo – secondo le informazioni archiviate da «qualcuno» in un «qualche» dove (soggetti e luoghi spesso sottratti all'individuazione: ulteriore elemento di crisi del sistema da disciplinare in sede giuridica) –, ma dell'identità psichica di ciascuno e secondo quello schema pre-riflettente che addirittura è in grado di prevedere le reazioni rispetto agli impulsi più della nostra razionalità. Questo complesso di dati classificati e archiviati ha una certa prossimità con l'Es freudiano che si sottrae all'io cosciente[3], finendo con il dare accesso al nostro inconscio. Il quantified self, inteso come misurazione in termini quantitativi (e qualitativi) della vita di ciascuno, è una realtà, così come il self tracking, e non è peregrino ipotizzare che

Diritto & Diritti ISSN 1127-8579

le aziende che detengono le informazioni conoscano di noi (e della nostra psiche) ben più di qualsiasi servizio informativo nazionale, e, aspetto ancora più inquietante, sono in grado di prevedere (più di noi stesssi) ogni nostra scelta con sempre maggiore dettaglio.

Si assiste dunque a un processo di deinteriorizzazione, laddove l'euforia illusoria della illimitata comunicazione digitale interconnessa si trasforma nell'ossimoro di una «dittatura della trasparenza» funzionale al suo sfruttamento in favore di pochi e ai danni dei molti. Le «tecnologie del sé»[4] dispiegano tutto il loro potenziale.

E' dunque l'autodeterminazione informativa a costituire la nuova frontiera nella tutela dei diritti. Un percorso che inizia da lontano, rispetto al quale già la Corte Costituzionale tedesca, nella storica sentenza del 15.12.1983, con profetica riflessione, ha elaborato dei significativi capisaldi in tema di elaborazione elettronica delle informazioni e della loro conservazione, rigettando il «sensitivity grading»[5] dei dati, pervenendo alla conclusione che «non c'è più nelle condizioni della moderna elaborazione dei dati alcun dato senza importanza» e, quanto più esso riguardi «eventi intimi» assume rilievo la «conoscenza del suo contesto di utilizzo». Pertanto, è illegittima una elaborazione «senza adeguato fondamento legislativo». Solamente «quando vi sia chiarezza» sugli scopi di utilizzo e sulle possibilità di connessione è possibile rispondere alla domanda circa l'ammissibilità di una limitazione: un passo in avanti rispetto alla teorizzazione del principio (Sphärenteorie) secondo cui l'intensità della tutela giuridica debba essere inversamente proporzionale alla «socialità» del comportamento. «E' incompatibile con il diritto all'autodeterminazione informativa un ordinamento… nel quale i cittadini non possano più sapere chi sa cosa sul loro conto, quando e in quale circostanza è venuto a saperlo».

Cybersecurity e data protection. I nuovi assetti normativi

In questo contesto di ingrediente progressione della vita digitale (nel mondo individuale e nella vita delle istituzioni) assumono un ruolo centrale – a tutela della libertà e della democrazia – la Cybersecurity (sempre più intesa come obiettivo strategico nelle politiche di intelligence) e la Data Protection. Obiettivi cui la stessa politica normativa europea è ormai orientata da alcuni anni, fino al più recente tentativo di trovare un assetto più efficace ed evoluto in quella che potremmo definire «trilogia» della sicurezza informatica, realizzata nel triennio 2016-2018, e destinata a compiersi sul piano dell'efficacia entro il maggio 2018, per mezzo di due regolamenti (Regolamento GDPR – General Data Protection –, n. 2016/679 e Regolamento sulla vita privata elettronica – entrambi di diretta applicazione, senza necessità di recepimento, a far data dal 25 maggio 2018) e di una Direttiva sulla sicurezza delle reti (cd. Direttiva NIS – Network Information Security – n. 2016/1148).

E' un punto di partenza, ma non di arrivo.

Le dinamiche della rete, segnate da un intrusivo sviluppo progressivo nella vita quotidiana, e

Diritto & Diritti ISSN 1127-8579

l'interconnessione dei sistemi rendono infatti improcastinabile, al di là delle previsioni normative più recenti la realizzazione di un assetto effettivo di tutele che – al passo con l'evoluzione tecnologica – garantisca, al tempo stesso, la sicurezza strategica delle infrastrutture e la protezione dei dati individuali (Data Protection) da un incontrollato sistema (non statuale e ageografico) di tracciatura e profilazione – sospeso tra analisi statistica e acquisizione di dinamiche dell'inconscio – . In questo contesto, assume valenza dirimente la nozione di «sovranità digitale» come snodo della necessaria tutela statuale in ambito nazionale e internazionale. In mancanza, la sottrazione dell'ambito a una tutela ordinamentale esporrà diritti fondamentali all'arbitrio di pochi, aprendo il passo al totalitarismo digitale.

Ormai lasciato alle spalle il web 2.0 e il 3.0, il web 4.0 (il vero spartiacque, in termini cibernetici, rispetto ai primi, verso una totale interoperabilità di tutti i sistemi di trasmissione delle informazioni) e, ancor di più, la rapida evoluzione verso il 5.0 (in cui l'interazione si estende anche alla sensorialità e, dunque, alla partecipazione emotiva del soggetto[6]), rappresentano delle frontiere che impongono scelte giuridiche, operative e strategiche di maggiore impatto, a tutela della persona nelle sue multiformi espressioni – e dunque nei sistemi ordinamentali frontalieri e transfrontalieri in cui si estrinsecano le relative attività.

Ha senso, pertanto, ed è inevitabile, transitare verso un nuovo assetto organizzativo della tutela, purché, tuttavia, si accresca sia il livello complessivo di consapevolezza, sia il grado di coinvolgimento – cd. information sharing – a ogni livello, di tutti i soggetti, pubblici e privati, siano essi, ai sensi della Dir. UE 2016/1148 (cd. Direttiva NIS), fornitori di servizi essenziali o fruitori di servizi digitali (in quanto tali chiamati ad incrementare le risorse investite nella sicurezza cibernetica, nonché ad individuare e formare figure intermedie preposte alla tutela della sicurezza, cd. consulenti per la sicurezza cibernetica).

La criticità del sistema appare infatti evidente, nel suo apparato, nell'ultimo anello della catena, che va rafforzato e reso per l'appunto resiliente, secondo quel grado individuato già a livello comunitario dalla Direttiva NIS: l'obiettivo è quello di assicurare la business continuity e la loro compliance con gli standard e i protocolli di sicurezza adottati a livello internazionale.

L'art. 346 del Trattato sul Funzionamento dell'Unione europea dispone che nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza; ne discende che la Direttiva 2016/1148 lascia impregiudicata l'autonomia di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati. Tale condizione di partenza potrebbe dunque costituire un ostacolo al pieno dispiegamento di azioni che nei fatti di rivelino efficaci, realizzando concretamente i profili programmatici intrinseci. Tuttavia, non può sottacersi la indifferibilità di misure ulteriori e rafforzate, volte a garantire gli obiettivi prefissi in sede comunitaria, che, si auspica, verranno compiutamente affrontati con l'integrale recepimento della Direttiva (che non può tardare).

Sulla medesima scia (quella della cybersecurity) in termini nazionali si inserisce – dal punto di vista istituzionale – l'approvazione del decreto (D.P.C.M. 17 febbraio 2017, cd. Decreto Gentiloni) in materia di

sicurezza cibernetica (che abroga il previgente D.P.C.M. 24 gennaio 2013) rende manifesta, in termini teleologici, prima ancora che organizzativi e normativi, la valenza strategica per la sicurezza nazionale di un sistema coordinato efficace e affidabile in grado di fronteggiare, con estrema competenza e immediatezza, emergenze sinora ritenute, nell'accezione comune, inusuali, se non marginali dal punto di vista operativo.

Il provvedimento, tentando il perseguimento degli obiettivi delineati dalla Direttiva cd. NIS (2016/1148 del Parlamento Europeo e del Consiglio del 6.7.2016) – il cui recepimento, al di là del termine del 9.5.2018 fissato all'art. 25, appare auspicabilmente improcastinabile alla luce della rapida e prevedibile evoluzione di eventi in grado di porre intrinsecamente in crisi gli ordinari assetti nazionali e interstatuali – segna il passo verso una nuova frontiera dal punto di vista metodologico e degli assetti organizzativi: il rafforzamento, nell'ambito operativo del programma nazionale di cyber security, del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) e del Nucleo di Sicurezza Cibernetica (NSC) – ricondotto nell'alveo del Dipartimento per le Informazioni per la Sicurezza (DIS) – rappresenta una risposta a una esigenza che supera definitivamente la rilevanza di natura meramente tecnica della funzionalità (e, per converso, vulnerabilità) delle reti, evidenziando il carattere strategico per la sicurezza nazionale dei sistemi sia pubblici sia privati, i quali andranno sottratti a qualsivoglia potenziale crisi indotta da attacchi esterni (profili sinora sottovalutati anche dall'opinione pubblica, la cui sensibilizzazione costituisce il primo step da affrontare nel quotidiano).

Il Decreto, nell'attribuire al direttore generale del DIS il compito di definire linee di azione che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico (onde eliminare le vulnerabilità anche con il "coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore"), dà sostanzialmente atto della natura degli interessi sottesi che, in quanto tali, protranno soggiacere evidentemente (e comprensibilmente), laddove si rendesse necessario a un regime giuridico rafforzato (anche sul piano della natura «classificata»), posto che (come ribadito dalla Corte Costituzionale, cfr. da ultimo sent. 40/2012) la classificazione della natura delle informazioni affonda la sua base di legittimazione nell'esigenza di salvaguardare supremi interessi riferibili allo Stato-comunità, ponendosi quale «strumento necessario per raggiungere il fine della sicurezza», esterna e interna, «dello Stato e per garantirne l'esistenza, l'integrità, nonché l'assetto democratico»: valori che trovano espressione in un complesso di norme costituzionali, e particolarmente in quelle degli artt. 1, 5 e 52 Cost. (C. Cost., sentenza n. 110 del 1998; in prospettiva analoga, sentenze n. 106 del 2009, n. 86 del 1977 e n. 82 del 1976).

La resilienza del sistema e le azioni positive

L'evoluzione normativa si muove nella consapevolezza che solo la resilienza del sistema interconnesso – cioè la capacità della rete a resistere ad attacchi esterni e ripristinarsi al livello di funzionalità iniziale a

Diritto & Diritti ISSN 1127-8579

cui è destinata – può garantire il transito verso un nuovo modello di tutela consapevole. Metro dell'efficienza è l'efficacia, ovverosia la sussumibilità dell'azione posta in essere entro parametri di concreta attuazione, suscettibili di «misurazione» quanto a conseguimento degli obiettivi, il cui esito primigenio è costituito dalla resilienza del sistema.

L'efficacia potrà essere originata (o, meglio, innescata) esclusivamente dall'introduzione di misure concrete che non solo intervengano sulle regole che sovrintendono – secondo i parametri definiti dalla direttiva – sia allo svolgimento dei processi di acquisizione di scambio e di conservazione dei dati (in possesso di soggetti pubblici e/o privati) sia, auspicabilmente, alle attività procedimentalizzate in sede telematica per mezzo di reali azioni positive volte al superamento del divario digitale sul piano della reingegnerizzazione dei processi[7]. I tentativi sul punto appaiono blandi. La problematica riapre – sotto nuovi e più evoluti profili – la tematica già nota da più di un decennio, del digital divide (a cui dovrebbe aggiungersi, in un'ottica di effettiva democratizzazione dei servizi anche l'assenza di una cultura adeguata alla evoluzione delle criticità sistemiche), oltre che il divario tra amministrazioni[8] e operatori economici privati; obiettivo quest'ultimo perseguibile solo nell'ambito di un processo di reingegnerizzazione dei processi[9] certamente non favorito dall'assenza di specifiche norme e, ancor prima, di concreti obiettivi.

Parallelamente, una tale condizione acuisce lo stridente contrasto con il precetto del secondo comma dell'art. 3 della nostra Carta fondamentale, se solo si considera che l'assenza di specifiche azioni positive in materia collide con il compito della Repubblica di «rimuovere gli ostacoli di ordine economico e sociale… che limitando di fatto la libertà e l'uguaglianza… impediscono l'effettiva partecipazione all'organizzazione politica, economica e sociale del paese». Infatti, posto che le nuove tecnologie favoriscono, soprattutto nell'ambito di un procedimento digitalizzato, la partecipazione diretta dei cittadini ai processi decisionali, l'obiettivo di una rete più efficiente e vicina all'utente – sul piano della sicurezza – potrà dirsi avviato solamente in un quadro di generale e concreto coinvolgimento di tutti gli «attori» della vita civile (sia chi è utente, sia chi progetta ed eroga pubblici servizi). Sarà così instaurato un processo di reale democratizzazione, senza vincoli di spazio e tempo, alimentato dalla progressiva riduzione dell'«asimmetria informativa»[10] tra poteri pubblici e cittadini[11]. A questo effetto, immediatamente percepibile, deve aggiungersi l'indiretto risultato di una «amministrazione partecipata», reso possibile dalla verificabilità costante, ad opera dei cittadini, dell'attività dei pubblici poteri.

In tale contesto muta radicalmente anche l'assetto tradizionale delle modalità di esercizio della funzione amministrativa[12] (intesa come espressione di potestas), considerato che viene a configurarsi un sistema in cui il baricentro non è più l'esercizio del potere (caratterizzato dall'autoritatività), ma il risultato, in termini di efficienza, di un servizio pubblico paritetico, realmente «universale»[13].

Si tratta, a questo punto, di «governare» il transito verso un nuovo modello.

L'argomento presuppone una chiara definizione normativa (non solamente teorica) dei confini che caratterizzano l'essenza degli istituti (di nuova formazione) e dei confini degli interessi da tutelare, che sono direttamente condizionati dal progressivo incedere della tecnologia, la cui velocità evolutiva

potrebbe rivelarsi ben più rapida dei testi normativi cristallizzati in previsioni inadeguate.

L’affidabilità e sicurezza delle reti come orizzonte dinamico

La pervasività dell’interconnessione della rete telematica passa attraverso un ulteriore consolidamento dell’“affidabilità e sicurezza” (locuzioni utilizzate dal legislatore europeo) del sistema.

Come evidenziato nel preambolo della Direttiva NIS, la portata, la frequenza e l'impatto degli incidenti a carico della sicurezza si incrementano per numero e qualità, sino a rappresentare non già solo una grave minaccia per il funzionamento delle reti e dei sistemi informativi, ma un concreto nocumento per l’«armonioso funzionamento del mercato» unico. Tenendo conto della dimensione transnazionale, le gravi perturbazioni di tali sistemi, intenzionali o meno, e indipendentemente dal luogo in cui si verificano, possono ripercuotersi sui singoli Stati membri e avere conseguenze in tutta l'Unione.

Occorrono ancora azioni volte ad attuare le finalità di quel gruppo di cooperazione che sia concretamente efficace e inclusivo, che, superando la fase meramente programmatica e organizzativa, passi attraverso misure positive che, da un lato realizzino l’obiettivo finale per cui tutti gli Stati membri possano disporre realmente di un livello minimo di capacità (dotandosi di una strategia volta a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi sul loro territorio) e, dall’altro, fissare normativamente, per gli operatori di servizi essenziali e ai fornitori di servizi digitali, ineludibili obblighi in materia di sicurezza e notifica volta a promuovere una cultura della gestione dei rischi e a garantire la segnalazione degli incidenti più gravi.

La cybersicurezza, in definitiva, oggi rappresenta un orizzonte dinamico cui tendere le vele con nuove misure efficaci e improcastinabili, superando la frontiera della tautologia e delle astratte affermazioni di principio prive di approfondimento operativo, avendo chiaro l’obiettivo che essa rappresenta un nucleo essenziale per la tutela dei diritti in un ambito significativamente caratterizzato da obiettivi strategici per la sicurezza nazionale e la competitività del paese nel contesto nazionale e transfrontaliero.

Inquadrata in questi termini la tematica, andrà analizzata la rapida evoluzione tecnologico-informatica che comporta un’altrettanto veloce obsolescenza delle norme che sovrintendono alla disciplina di materie correlate alle tecnologie dell’informazione e della comunicazione. Esse necessitano di costanti revisioni e aggiornamenti, oltre che di integrazioni, anche per sedimentare un substrato giuridico per tutte le attività finalizzate alla protezione cibernetica e alla responsabilizzazione degli amministratori e degli utenti delle operazioni compiute sui sistemi loro assegnati.

Il profilo più complesso – come del resto già posto in evidenza nel Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica predisposto dalla Presidenza del Consiglio nel marzo 2017 – è rappresentato dalla valutazione dell’allineamento tra l’attuale assetto giuridico interno e le dinamiche di

sviluppo legate all'innovazione tecnologica, esaminando l'eventualità di interventi normativi e tenendo conto delle best practices internazionali. In questo senso, occorre finalizzare il quadro normativo relativo alle infrastrutture critiche nazionali informatizzate, pubbliche e private, volto alla definizione dei criteri per la loro individuazione tenendo conto anche di quelli stabiliti per i settori rientranti nel campo di applicazione della Direttiva NIS

Altro campo di azione è costituito dalla semplificazione e dalla armonizzazione degli adempimenti e degli obblighi gravanti sulle amministrazioni e sugli operatori economici privati con lo scopo di incrementare l'efficacia delle comunicazioni in tema di data breach e incident notification nonché perseguire l'effettività e l'efficienza di politiche e di misure di sicurezza.

Come ricordato dal Presidente delll'Autorità Garante per la Protezione dei Dati Personali[14] In questi anni il cybercrime ha superato il mercato del narcotraffico a fronte di un danno stimato di oltre 500 miliardi di dollari al business mondiale. Secondo le stime, il 72% degli attacchi verificatisi nell'ultimo anno a livello globale sarebbe stato effettuato a fini estorsivi o di sfruttamento di dati personali. Le infrastrutture critiche hanno subito un incremento del 15% di attacchi rispetto allo scorso anno. Sarebbero cresciuti del 117% gli attacchi riconducibili ad attività di cyberwarfare, che utilizzano canali telematici per esercitare pressione su scelte geopoliticamente rilevanti, mentre il phishing avrebbe raggiunto punte di incremento del 1.000% - a conferma del fattore umano (inesperienza degli utenti) che condiziona in misura preponderante le falle della sicurezza informatica.

Molte delle amministrazioni centrali e periferiche dello Stato, prima ancora (e forse molto più) delle reti private aziendali, sono esposte a una intrinseca vulnerabilità legata spesso, in un contesto di disomogeneità totale, a obsolescenza dei sistemi o non adeguata percezione del rischio da parte dei centri decisionali preposti, destinata – per effetto dell'interconnessione – a riverberarsi sulla tenuta complessiva dello spazio cibernetico che oggi è il vero (forse unico) centro nevralgico delle dinamiche economico-politiche. Ciò implica che gran parte degli sforzi normativi in ambito europeo e, di riflesso, nazionale, finirebbero con il rivelarsi misure del tutto inefficaci in assenza di specifici investimenti umani e finanziari volti a rendere effettivo il sistema di resilienza.

In questo ambito, in cui le relazioni ostili, interne ed esterne agli stati, si svolgono con incipiente, e poi crescente, incedere nella realtà digitale è inevitabile proporsi di estendere a quest'ultima gli strumenti per la difesa degli equilibri di natura internazionale dalle tradizionali aggressioni, in presenza di serie minacce che si propongono nelle rinnovate vesti del cyberwarfare (guerra cibernetica) e dell'hactivism in termini di attività antagonismo politico in forma digitalizzata.

La sicurezza cibernetica come «bene comune»

C'è un nucleo essenziale di dati rispetto al quale non è possibile abdicare quanto a tutele. Ne va della

libertà di tutti e della tenuta democratica delle istituzioni.

La Direttiva 1148/2016 (NIS) sulla sicurezza delle informazioni e delle reti sottende una nozione di sicurezza cibernetica intesa come «bene comune», in quanto la tutela è riposta sul carattere di interdipendenza dei singoli sistemi all'interno del sistema, e, ancor prima sulla condivisione. In questo contesto assume carattere dirimente (come evidenziato nel documento recante la Strategia UE per la cybersicurezza) un corretto reinquadramento della nozione di sicurezza digitale, avendo ben chiaro l'ambito di azione diviso tra due spazi autonomi e interdipendenti al tempo stesso: la sicurezza cibernetica da un lato e quella informatica dall'altro – laddove nel primo caso prevale la dinamica relazionale della rete – ; avendo ben chiaro che la protezione dell'infrastruttura deve puntare innanzi tutto sugli aspetti di interconnessione.

La proposta di Regolamento europeo sulla vita privata digitale (2017/0003 COD - rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE - «Regolamento sulla vita privata e le comunicazioni elettroniche» -) pone in rilievo l'esigenza di dare concreta attuazione ai principi fissati dall'art. 8, § 1, della Carta Fondamentale dei Diritti dell'Unione Europea e dall'art. 16, § 1, del Trattato di Funzionamento dell'Unione Europea in uno spazio sinora non adeguatamente tutelato in presenza di una repentina evoluzione tecnologica (es. servizi di telecomunicazione cd. OTT, Over The Top, tra cui messaggistica istantanea, posta elettronica on web, servizi di voice over ip, spesso veicolati per mezzo di hotspot privati in spazi aperti al pubblico). Si pensi al contenuto delle comunicazioni elettroniche che può rivelare informazioni altamente sensibili in merito alle persone fisiche coinvolte nella comunicazione, alle loro esperienze personali ed emozioni, alle condizioni mediche, alle preferenze sessuali e alle opinioni politiche, «la divulgazione delle quali potrebbe tradursi in un danno personale e sociale, in una perdita economica o nel semplice imbarazzo» (considerando n. 2 dello schema di Regolamento 2017/0003 COD). Analogamente, i metadati derivati dalle comunicazioni elettroniche possono anch'essi rivelare informazioni estremamente sensibili e personali, che includono i numeri chiamati, i siti web visitati, la geolocalizzazione, l'ora, la data e la durata di una chiamata effettuata, consentendo di trarre conclusioni precise relativamente alla vita privata delle persone coinvolte nella comunicazione elettronica, come le loro relazioni sociali, le loro abitudini e attività quotidiane, i loro interessi, gusti.

Non ha senso predisporre delle forme di tutela astratta senza avere chiaro il processo di superamento del monadismo telematico verso un adeguato grado di coscienza dell'interoperabilità dei sistemi, al fine di predisporre strumenti di tutela in grado di conciliare la nozione di «bene comune» (che pervade l'intrinseca natura della rete) con una realtà ben più complessa che, anche se non inquadrabile in termini di diritti dominicali, finisce con il ricadere nella esclusiva disponibilità di quei soggetti, privati e pubblici, nonché Stati, i quali controllano i singoli segmenti attraverso i quali vengono veicolati i dati e finiscono con l'esercitare il dominio assoluto su nodi e tecnologie attraversati dalle comunicazioni.

Diritto & Diritti ISSN 1127-8579

Governance dei sistemi di rete e sovranità telematica. Rilievi conclusivi

La ricerca di adeguate forme di tutela reca in sé l'ineludibile esigenza di analizzare il consolidamento di adeguati meccanismi di governance telematica delle reti e dei relativi sistemi, con chiare e puntuali assunzioni di responsabilità pubbliche in ambito nazionale, europeo e transfrontaliero, che garantiscano effettività democratica nella tutela dei dati e delle informazioni, sulla base della consapevolezza che, diversamente, la dipendenza incondizionata (e spesso inconsapevole) da chi ha la titolarità delle infrastrutture rende dipendenti e vulnerabili al tempo stesso dalle azioni di questi ultimi.

La sicurezza delle reti finisce dunque per correlarsi sempre più alla nozione di sovranità telematica, che richiede un adeguato grado di coscienza e di regolazione condivisa (che temperi la natura a-geografica della rete con una riconducibilità a degli ordinamenti giuridici che garantiscano effettività nella tutela dei diritti e degli interessi coinvolti), in assenza della quale è messa in pericolo la democrazia. Un'opera che va oltre i singoli confini (nazionali o europei) entro i quali il rischio connesso di crisi della rete mira a relegare ogni iniziativa e ben al di là delle ordinarie azioni positive di sicurezza delle infrastrutture, che eventualmente – secondo il disegno ordinario di cybersecurity – si svolgono limitatamente ai nodi interni di interscambio internet ixp prevenendo l'ipotesi di accesso illecito (interno o esterno: v. casi Hacking Team, o Datagate a solo titolo esemplificativo) ai dati veicolati attraverso tali infrastrutture rafforzandone la capacità di resilienza. Esigenza tanto più immanente in ragione del peso specifico assunto dal contenuto delle attività di profilazione dei singoli (spesso inconsapevoli), che finisce con il superare la nozione (e la funzione) originaria dei Big Data, oppure il senso stesso dei limiti alla Data retention imposti dal principio di proporzionalità, laddove si consideri che il punto di crisi non è correlato, in termini di attività strategica e di prevenzione, al signal intelligence, quanto alla detenzione impropria di quei dati da parte di terzi per effetto delle distorsioni indotte lungo la catena di distribuzione degli stessi (ragione per cui ben può condividersi il tentativo volto, anche in sede normativa, a ridurre la «superfice» potenziale di attacco e concentrare la frammentazione delle informazioni).

Siamo oggi in una fase di svolta: non è più sufficiente perseguire una politica di neutralizzazione del rischio fronteggiando le criticità delle misure di sicurezza nell'ambito dei nodi interni, riducendo, e – se possibile – tentando di azzerare, i rischi di permeabilità mediante il solo ricorso a strumenti normativi e metodologie tecniche, per quanto adeguati essi possano rivelarsi.

Sarebbe infatti sufficiente l'instradamento dei flussi telematici verso aree grigie, o peggio ancora franche (sottratte per l'appunto a qualsivoglia forma di sovranità telematica, che assicuri tutela dei dati nel rispetto delle libertà coinvolte), per annichilire al tempo stesso ingenti investimenti umani e finanziari operati nel campo della cybersecurity, arrecare incalcolabili danni alla tenuta strategica del sistema, e porre in pericolo libertà e democrazia.

Diritto & Diritti ISSN 1127-8579

L’obiettivo si evolve dunque in ambiti multiformi ed è su quello che l’attività di intelligence può compiere il salto qualitativo. La tutela dei dati si deve muovere in primo lungo lungo il solco biunivoco (già delineato dal Regolamento GDPR 689/2016) by design e by default, cioè sin dalla fase di progettazione e poi durante il suo svolgimento operativo, ma prima ancora deve ricondursi a una fase di responsabilizzazione in ambito pubblico internazionale che necessariamente passi attraverso la predisposizione di adeguate misure di governance digitale, a tutela della libertà di tutti.

E’ questo il senso della nozione di sovranità digitale che, in assenza di una presa di coscienza del suo ruolo non adeguatamente delineato, né tanto meno «positivizzato» in ambito internazionale, e della predisposizione delle necessarie misure di intervento, finirà con il tradursi in una riduzione della sovranità reale a favore di pochi, ai danni della libertà degli individui e delle collettività che ne rappresentano i centri esponenziali.

Diversamente, l’illusione della trasparenza digitale illimitata finirà con il trasformarsi in vuoto simulacro sottratto a ogni forma di tutela statuale in sede nazionale e internazionale e, dunque, in un campo libero esposto a forme di pericoloso, e spesso subdolo, totalitarismo digitale ai danni della libertà di tutti.

[1] **Byung-Chul Han,** Psicopolitica. Il neoliberalismo e le nuove tecniche del potere, traduzione di Federica Buongiorno, 2016: «L'accelerazione della comunicazione favorisce la sua emozionalizzazione, dal momento che la razionalità è più lenta dell’emotività. La razionalità è, in un certo senso, senza velocità. Per questo l'impulso acceleratore conduce alla dittatura dell’emozione”. E mentre “gli oggetti non possono essere consumati all'infinito, le emozioni invece sì. Le emozioni sono dispiegate al di là del valore d'uso. Quindi si apre un nuovo campo di consumo con caratteristiche infinite». Con riferimento ai Big Data si arriva al paradosso per cui questi dati non sono “confessioni

estorte con la tortura”, piuttosto, secondo Han, «si verifica una spoliazione volontaria. Il Grande Fratello ha un aspetto amichevole. L'efficienza della sorveglianza risiede nella sua bontà». Ma questi dati non sono «confessioni

estorte con la tortura”. Piuttosto, dice Han, “si verifica una spoliazione volontaria. Il Grande Fratello ha un aspetto amichevole. L'efficienza della sorveglianza risiede nella sua bontà».

[2] Jeremy Bentham, Panopticon ovvero la casa d’ispezione , a cura di M. Foucault e M. Perrot, trad. it. di V. Fortunati, Venezia, 1983.

[3] **Byung-Chul Han**, op. cit., p. 76.

[4] Secondo la definizione di **Michel Focault**, Tecnologie del sé. Un seminario con Michel Foucault, a cura di **L.H. Martin** e altri, Torino, 1992.

Diritto & Diritti ISSN 1127-8579

[5] La teoria secondo cui cui le informazioni personali sono suscettibili di differente disciplina e hanno un diverso grado di pericolosità in rapporto ai profili della personalità cui si riferiscono, cosicché, una volta classificate, la relativa regolamentazione andrà adeguata alla loro categorizzazione contenutistica.

[6] così **Aijt Kambil**, What is your Web 5.0 strategy?, in Journal of Business Strategy, Vol. 29 Iss: 6, pp.56 – 58: «Web 5.0 a sensory emotive space where we are able to move the web from an emotionally flat environment to a space of rich interactions».

[7] Cfr. **Alessandro Biamonte**, L'amministrazione digitale e la digitalizzazione procedimentale. Verso un nuovo esercizio della funzione. Problematiche e prospettive, in Studi sul procedimento e sul provvedimento amministrativo, Aa.Vv., Bologna, 2007, pp. 237 – 268.

[8] L'art. 9 (Alfabetizzazione informatica dei cittadini) del Codice dell'amministrazione digitale, D.Lgs. 82/2005, dispone che «Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni" e l'art. 14, comma 3, che «Lo Stato, ...previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale». Entrambe disposizioni di carattere meramente programmatico, in ordine alle quali il Consiglio di Stato nel citato parere n. 31/2006 ribadisce la necessità di specifiche e concrete azioni che «richiedono una adeguata copertura finanziaria e amministrativa».

[9] V. in tema di reingegnerizzazione dei processi (Business Process Reenginering) www.cnipa.gov.it: una modalità di cambiamento organizzativo caratterizzata da un intervento su uno o più processi di servizio tra loro correlati; è guidata dagli obiettivi strategici dell'organizzazione individuati in partenza (nel nostro caso norma cardine è l'art. 97 Cost. da cui fare discendere tutti gli altri obiettivi); non è vincolata, nell'individuazione delle nuove soluzioni, ma muove dalla situazione esistente secondo un approccio dinamico mirando ad un cambiamento radicale che assicuri un "salto" nei risultati; è verificato attraverso un sistema di «metriche» (caratteristica quest'ultima che consente di verificare progressi o decrementi operativi, al fine di operare correttivi. Essa presuppone dunque l'individuazione dei processi primari di una organizzazione legati al core business («missione istituzionale») della singola amministrazione pubblica, che creano "valore" riconosciuto all'esterno dai clienti e che pertanto sono critici per avere successo. Su tali processi viene effettuata una diagnosi volta ad individuare le aree di criticità e di possibile miglioramento (attività nullo o scarso valore aggiunto che possono essere eliminate, flussi operativi irrazionali, frammentazione di responsabilità e operatività, carenze informative...) e a definire i valori obiettivo in termini di «metriche di prestazione». La diagnosi costituisce il punto di partenza per una vera e propria riprogettazione che, come si è detto interverrà in genere su tutte le componenti dando origine a un insieme di interventi operativi tra loro correlati (ridefinizione dei flussi, redistribuzione delle responsabilità, realizzazione nuovi sistemi informativi e utilizzo di nuove tecnologie, formazione e

incentivazione del personale).

[10] Così **Alfonso Masucci**, Informatica pubblica, in Dizionario di diritto pubblico, diretto da Sabino Cassese, IV, Milano, 2006, p. 3119; Id., Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte, Torino, 2011, pp. IX-128, dove la riflessione viene ricondotta allo schema logico secondo cui i programmi informatici costituiscono insiemi di istruzioni basate sulla logica condizionale del "Se…Allora". Pertanto, un programma potrà contenere ogni tipo di istruzione, incluse quelle derivabili da norme giuridiche, nella misura in cui queste possano essere rese secondo la logica del "Se…Allora". Ne deriva che "un testo normativo per poter essere applicato mediante computer […] deve essere formulato attraverso concetti giuridici precisi […] Quando ricorrono concetti giuridici indeterminati ovvero quando i concetti (indeterminati) sono caratterizzati da una molteplicità di significati con essi compatibili […] ricorre uno 'spazio valutativo' che l'amministrazione deve riempire di volta in volta [e in cui] non è possibile l'applicazione della normativa mediante computer" (p. 91).

[11] Sul processo di democratizzazione dei processi decisionali: v. **Stefano Rodotà**, Tecnopolitica, Bari, 2004, p. 27 ss.; **Anna Pirozzoli**, La libertà di riunione in Internet¸ in Diritto dell'informazione e della informatica, 2004, p. 595 ss. .

12] Cfr., sul concetto originario di funzione, Aldo Piras, Discrezionalità amministrativa, in Enc. del Diritto, XIII, Milano, 1964, p. 65 ss. . La funzione, in quanto qualificata dall'attribuzione al suo titolare di un munus, ovvero officium, viene originariamente ascritta al genere delle «potestà», identificandosi con una condizione che viene «conferita» affinché si eserciti in considerazione di un interesse quanto meno non esclusivamente proprio, o di natura oggettiva. L'evoluzione dottrinale conduce poi ad inquadrare l'attività amministrativa e la rilevanza della funzione in un quadro complessivo in cui il ruolo cardine è svolto dall'esercizio della discrezionalità, in ragione dell'esigenza dell'ordinamento di vincolare l'attività «alla sola necessità di soddisfare gli interessi risultanti dalla predeterminazione delle competenze o dalla descrizione normativa dei fatti dell'azione» (così Piras, Discrezionalità amministrativa, op. cit., p. 78).

[13] Universalità intesa in senso verticale – nei rapporti tra i cittadini e la P.A. (che garantisce l'accesso a servizi di massima qualità a condizioni raggiungibili per tutti) – e orizzontale – tra tutte le amministrazioni nazionali e internazionali (in un contesto paneuropeo e transfrontaliero).

Quanto al primo punto, universalità verticale, tutte le pubbliche amministrazioni sono tenute a collaborare «per integrare i procedimenti al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione» (art. 63, comma 3, D.Lgs. 82/2005). Ciò dopo avere prestato attenzione all'integrazione dei procedimenti e alla loro efficienza (mirando alla soddisfazione degli utenti: art. 63, comma 2). Cfr. Alfonso Masucci, Erogazione on line dei servizi pubblici e teleprocedure amministrative, in Diritto pubblico, n. 3/2003, pp. 991 e ss. . Qui l'autore delinea: il principio di adattamento, che «deve essere inteso nel senso che l'erogazione del servizio deve adeguarsi costantemente e tempestivamente ai bisogni degli utenti e alle esigenze della generalità»; il principio di continuità, che di regola comporta l'obbligo di erogazione del

servizio nei normali orari di apertura degli uffici pubblici, mentre, nella dimensione erogativa di rete, va invece configurato come «permanenza» e come «disponibilità immediata del servizio… Attraverso la rete è possibile l'accesso al sito in qualsiasi ora e da qualsiasi luogo»; il principio di eguaglianza, da interpretarsi nel senso di eguale accessibilità ai servizi erogati dall'amministrazione da parte di tutti i privati (cittadini e/o imprese), indipendentemente dalla localizzazione geografica degli utenti, nonché dalla loro condizioni economico-sociali. Si realizza così una «continuità del servizio», il cui concetto assume il significato di disponibilità permanente ed immediata dello stesso: v. Alfonso Masucci, Informatica pubblica, op. cit, p. 3121.

In ordine al secondo argomento, universalità orizzontale, è fondamentale l'introduzione di sistemi che siano realmente in grado di operare tra loro. Di qui molteplici progetti nazionali e internazionali e altrettanti atti programmatici, tra i quali emergono le raccomandazioni contenute nelle Comunicazioni sull' e-Europe [8.12.1999 COM (1999) 687; 28.5.2002 COM (2002) 263].

Centrale in entrambi i casi è l'interoperabilità, che si estrinseca nel complesso di tutti i presupposti che consentono ai sistemi di «dialogare» tra loro.

L'interoperabilità va in ogni caso tenuta distinta dall'interconnessione che attiene esclusivamente agli aspetti hardware della connessione e al software di comunicazione – prius logico di una rete tra le amministrazioni che possa «interoperare» -. Aspetti entrambi assorbibili nell'ambito del progetto del Sistema Pubblico di Connettività (SPC), che si attende, tuttavia, alla prova dei fatti.

[14] Audizione del Presidente del Garante per la protezione dei dati personali, sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico innanzi alle Commissioni Affari Costituzionali e Difesa della Camera del 7.3.2017.

https://www.diritto.it/tutela-dei-diritti-mondi-intrusivi-digitali/

Diritto & Diritti ISSN 1127-8579