Rivista Semestrale

Gennaio – Giugno 2019

N. 1/2019

Data Protection Law

Diritto delle nuove tecnologie, privacy e protezione dati personali

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it

Diretta da Elio Errichiello

www.dataprotectionlaw.it

Indice.

LIVIA AULINO, Giustizia ed Intelligenza artificiale tra rischio da sviluppo e principi etici e deontologici.

Pag. 3

GIULIO RICCIO, La tutela del copyright nella Società dell'Informazione.

Pag. 12

ROSANNA CELELLA, Le nuove frontiere dell'accesso generalizzato e i confini della normativa sulla protezione dei dati personali.

Pag. 22

RITA DI MARCO, Machine learning e giustizia penale.

Pag. 32

SERGIO GUIDA, Il Cybersecurity Act sarà presto lo scudo europeo a difesa di rischi e minacce informatici sempre più insidiosi e sofisticati, che richiedono regole globali.

Pag. 37

GIUSTIZIA ED INTELLIGENZA ARTIFICIALE TRA RISCHIO DA SVILUPPO E PRINCIPI ETICI E DEONTOLOGICI.

Di Livia Aulino

SOMMARIO. 1. Le origini dell'intelligenza artificiale. – 2. Soggettività giuridica digitale e decisione. 3. Intelligenza artificiale e sistema giurisdizionale. – 4. Intelligenza artificiale e sistema legale – forense. – 5. Profili etici e deontologici.

The concept of artificial intelligence has very ancient origins, yet, in recent years, due to technological evolution, studies on the subject have advanced. In particular, the application of intelligence to the legal - jurisdictional sector can concern different points of view, up to the point of simulating perfectly human intelligence having the ability to "predict" the outcome of a judgment.

In this context, the relevance of ethics and deontology emerges, which represent the emblem of the ontological distinction between human agents and artificial inference.

1. Le origini dell'intelligenza artificiale.

Il termine "intelligenza artificiale" (meglio identificato con l'acronimo I. A. o A. I.) è quella parte della scienza dei computer riguardante lo studio e la creazione di sistemi[1] progettati in modo da avere quelle stesse caratteristiche che associamo all'intelligenza umana: comprensione del linguaggio, capacità di imparare, capacità di risolvere problemi e così via[2].

[1] Si tratta di sistemi dotati di un certo grado di autonomia che gli permette di compiere azioni e raggiungere obiettivi specifici; essi comprendono sia i *software*, che agiscono nel mondo virtuale, sia sistemi incorporati in dispositivi *hardware* (es. auto a guida autonoma, droni, ecc.).

[2] M. IASELLI, *Informatica e nuove regole per la produzione del diritto*, in *Diritto delle nuove tecnologie informatiche e dell'Internet*, (a cura di) CASSANO G., 2002, p. 1467 ss.

In realtà, il termine "intelligenza artificiale" esiste già da diversi secoli, essendo stato oggetto di studi filosofici[3], letterari[4] e da ultimo cinematografici[5]; in generale, l'uomo ha da sempre cercato di sviluppare delle macchine che potessero sostituirlo nelle attività più pesanti.

Dal punto di vista tecnico, invece, si tratta di un concetto di recente sviluppo, la cui cronostoria può essere tracciata in tre distinte fasi.

La prima fase comprende un periodo molto ampio, a partire dall'origine del concetto di intelligenza artificiale, nel 1623[6]. Eppure, il merito di aver coniato l'espressione "intelligenza artificiale" viene attribuita, da alcuni, ad Alan M. Turing, matematico inglese, che nel 1950, pubblicò il saggio *«Computing Machinery and Intelligence»*[7]*;* secondo altri, all'informatico statunitense J. Mc Carthy, che nel 1956, svolse un convegno sullo sviluppo dei sistemi intelligenti al Dartmouth College, nel New Hampshire[8].

La seconda fase si è sviluppata tra gli anni '80 e '90 del 1900, ed è stata caratterizzata per lo svolgimento dei primi studi giuridici su sistemi esperti ed agenti intelligenti[9].

[3] Numerosi studiosi, quali Blaise Pascal e Claude Elwood Shannon, hanno affrontato la tematica.

[4] Isamon ha ideato le leggi della robotica, che ad oggi rappresentano il punto di riferimento, anche normativo.

[5] Si pensi ai film: 2001 *Odissea nello spazio* (1968); *Westworld* (1973); *Tron* (1982); *Blade Runner* (1982); *Terminator* (1984); *L'uomo bicentenario* (1999); *Matrix* (1999 – 2003); *A.I. - Intelligenza artificiale* (2001); *Io, Robot* (2004); *Her* (2013); *The Machine* (2013); *Trascendence* (2014); *Ex Machina* (2015).

[6] In quell'anno, infatti, Willhelm Sickhart elaborò una macchina in grado di fare calcoli a sei cifre, con il supporto umano.

[7] L'articolo di Turing rappresenta il punto di svolta decisivo negli studi sulla relazione corpo-mente e sull'intelligenza artificiale. Da qui nasce l'idea di realizzare un computer simile al cervello umano fino alla prospettiva di avere un'intelligenza senza copro. Si sviluppa così la moderna robotica. I robot (lavoro forzato) stanno acquisendo crescenti capacità in alcune specifiche attività umane; oggi si parte dal più esteso concetto di agenti autonomi: termine che viene utilizzato per comprendere molti tipi di agenti artificiali in grado però di assumere autonomamente decisioni senza la direzione di un essere umano. All'interno di questa categoria sono inclusi: robot, droni, agenti *software* puramente digitali.

[8] Il termine i. a. nasce nel 1956 durante la conferenza di Darthmount: la ricerca aveva come scopo quella di realizzare un i. a. che riproducesse l'intelligenza umana, e quindi che fosse dotata di: un ragionamento logico; comprensione del linguaggio; percezione dell'ambiente esterno; capacità di movimento ed esplorazione; intelligenza emotiva; ragionamento morale.

[9] In quegli anni, alcuni studiosi, quali V. Frosini, E. Giannantonio, R. Borruso, si impegnarono per coniugare i principi dell'intelligenza artificiale con le ricerche evolute svolte dalle banche dati giuridiche.

In questo stesso periodo, un gruppo di magistrati[10], realizzò uno strumento meglio conosciuto come Italgiure, idoneo ad organizzare, in modo automatizzato, le massime della Corte Suprema di Cassazione, attraverso l'uso di un dizionario specifico della lingua italiana definito thesaurus[11]. Le ricerche del tempo produssero considerevoli risultati teorici, che però mal si conciliarono con la limitata potenza di calcolo dei computer e la conseguente inadeguatezza nell'affrontare la complessità degli algoritmi.

Dal 2010 in poi, è iniziata la terza fase, con lo sviluppo della potenza di calcolo dei pc e l'avvento di nuovi fenomeni: i Big Data; le machine learning[12]; i cloud supercomputing.

2. Soggettività giuridica digitale e decisione.

Il progressivo sviluppo della tecnologia robotica porta inevitabilmente ad un ripensamento della qualificazione giuridica dei robot, che non possono più essere considerati meramente oggetti al servizio dell'attività umana, ma divengono sempre più veri e propri agenti.

Il progresso tecnologico degli ultimi dieci anni ha reso i robot sia capaci di svolgere attività, tipicamente erano svolte dagli uomini, sia di acquisire capacità cognitive avanzate, che gli permettono di adattarsi e di interagire con l'ambiente in cui operano con una componente di imprevedibilità. L'elemento dell'imprevedibilità, però, comporta alcune problematiche dal punto di vista della responsabilità civile contrattuale ed extracontrattuale.

A tal proposito, nel febbraio 2017, il Parlamento UE ha approvato una risoluzione[13], concernente norme di diritto civile sulla robotica, secondo cui i robot dovranno, sempre più, rispettare le norme vigenti; questa considerazione, dal punto di vista giuridico, presuppone che i robot siano legalmente responsabili per le proprie attività.

---

[10] Tra cui lo stesso R. Borruso, A. Falcone, V. Novelli e U. Berni Canani.

[11] L'uso del *thesaurus* costituisce il primo serio passo di "intelligenza artificiale" realizzata col computer in un ambito non numerico.

[12] *Machine learning* è una branca dell'i. a., che permette ai computer di eseguire *task* cognitivi senza essere programmati esplicitamente.

[13] Risoluzione del Parlamento europeo, del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2013 (INL).

Eppure, contemplare i robot come soggetti autonomi, implica che essi debbano necessariamente essere regolati da norme che prevedono una responsabilità per azioni o omissioni degli stessi, laddove le cause di responsabilità non possano essere ricondotte ad un soggetto specifico (es. fabbricante, proprietario, utilizzatore)[14]. La prospettiva è la creazione di uno tertum status giuridico specifico per i robot, con la prospettiva di classificare gli automi come «persone elettroniche» titolare di diritti e doveri, diversi dalla persona fisica e giuridica e responsabili delle proprie azioni.

3. Intelligenza artificiale e sistema giurisdizionale.

Preliminarmente, si rileva che l'algoritmo[15] consiste nell'insieme delle istruzioni che compongono un programma[16]. Ne consegue che il computer, munito di adeguato software, può svolgere qualsiasi attività consentita da questo.

Attualmente, si possono tradurre in algoritmo tante operazioni matematiche quante sono le attività dell'uomo; l'algoritmo quindi, ha il merito di costituire un punto d'incontro tra due culture, da sempre considerate (erroneamente) opposte: l'umanistica e la scientifica.

Nessun problema si pone con riguardo agli strumenti di ausilio ai fini delle decisioni del giudice. Infatti, in tale ambito, sono già stati sperimentati in tutto il mondo casi di sistemi di intelligenza artificiale in grado di coadiuvare il ruolo del Giudice, soprattutto nei sistemi giuridici di common law.

Negli Stati Uniti, tre ricercatori, basandosi sugli sviluppi dell'apprendimento automatico nella scienza della previsione giudiziaria e sull'analisi della giurisprudenza della Corte Suprema degli Stati Uniti, hanno realizzato un sistema di machine learning per prevedere il comportamento della Corte Suprema in un contesto generalizzato[17].

Altresì, in Argentina, il procuratore generale nel contenzioso amministrativo della città di Buenos Aires, Juan Gustavo Corvalàn, nel corso di un Convegno svoltosi in Italia nel 2018, ha raccontato di aver contribuito alla realizzazione di «Prometea»,

[14] In generale, sarebbe auspicabile un sistema di presunzione della responsabilità del produttore/o onere della prova sul produttore, ciò al fine di garantire maggiormente la tutela al consumatore.

[15] Il termine deriva dal nome del matematico arabo, Al-Khuwarizmi, vissuto circa mille anni fa, considerato il padre dell'algebra.

[16] Il *software* non è altro che lo sviluppo di un algoritmo.

[17] A tal proposito, sono stati analizzati 240.000 votazioni e 28.000 casi in quasi due secoli (1816-2015). Usando questo modello predittivo lo studio ha ottenuto un'accuratezza del 70,2% a livello di decisioni giudiziari e del 71,9% a livello di voti espressi dai Giudici.

un sistema di intelligenza artificiale che consente la soluzione di casi giudiziari a struttura semplice e ripetitiva in uno spazio temporale di pochi secondi[18].

Lo stesso software è attualmente utilizzato anche nella Corte interamericana dei diritti umani, ove è stata aumentata l'efficienza fino al 143%. Una sperimentazione è in corso anche presso il Consiglio di Stato a Parigi.

Diverso è il discorso, se tra le attività umane, traducibili in algoritmo, comprendiamo anche quella di decisione di una causa (civile o penale). Ci si chiede, quindi, se la funzione "predittiva" dell'intelligenza artificiale possa consistere nella capacità di "prevedere" l'esito di un giudizio.

La normativa vigente, nel fare riferimento al diritto di ogni persona che la sua causa sia esaminata da parte di un "tribunale indipendente ed imparziale" (ex art. 6, comma della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali) e nel prevedere che ogni processo debba svolgersi davanti ad un "giudice terzo e imparziale" (ex art. 111, 2 co., Cost.), esclude tale possibilità. Inoltre, l'art. 220, 2 co., c.p.p., infatti, sancisce che non è ammessa la perizia per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche dell'imputato indipendenti da cause patologiche; altresì, l'art. 14 del D. lgs. n. 196/2003 (cd. codice privacy), trasfuso nell'art. 22 del recente Regolamento UE n. 2016/679, in materia di protezione dei dati personali, che stabilisce che nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano possa essere ondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

Eppure, la Carta etica europea del 2018 ammette l'uso, sotto il controllo umano, dell'intelligenza artificiale nei sistemi di giustizia penale. Ciò significa che ad un computer potrebbe essere demandata, sia la decisione finale sulla colpevolezza o meno di un imputato o la quantificazione dell'eventuale pena da irrogare, che la soluzione di specifiche questioni costituenti presupposto di tale decisione.

[18] Attualmente questo sistema trova applicazione in oltre il 52% dei casi sottoposti alla Corte Superiore di giustizia di quella città, con un tasso di successo (parametrato alle soluzioni poi effettivamente adottate dai magistrati) del 96% dei casi.

Grazie all'utilizzo di questo sistema, a supporto della Corte, 1.000 casi possono essere trattati nell'arco di 7 giorni, mentre manualmente sarebbero necessari 83 giorni di lavoro.

Il tema della prevedibilità delle decisioni è già da tempo al centro di un vivace di un dibattito dottrinale. In particolare, il fatto che sia possibile prevedere l'orientamento decisionale di un giudice è stato ritenuto, per certi aspetti, positivo nella misura in cui può servire a migliorare il livello di efficienza della giustizia ma, sotto altri, nega per il rischio di riduzione ad una gestione automatizzata di affermazioni standardizzate[19].

A questo punto, occorre precisare che è algoritmizzabile solo ciò che è razionale; pertanto, atteso che tutta la sfera dell'attività psichica irrazionale, in quanto tale, non risponde a regole, l'uomo non potrà mai essere sostituito da un computer nelle manifestazioni della sua creatività, nella fantasia, nella sfera dei sentimenti, cioè nell'affettività, desiderio di conoscenza e di novità, in tutte queste attività "il computer potrà essere usato non per sostituire l'uomo, ma solo per studiarlo meglio"[20]. Inoltre, è opportuno rilevare la differenza sussistente tra i concetti di "Sense" e di "Sensibility", allorquando la macchina sente, ma l'intelletto dell'uomo (giudice) percepisce; l'uomo, infatti, è dotato della sensibilità che alle macchine manca, ed indispensabile per emettere un giudizio.

4. Intelligenza artificiale e sistema legale - forense.

Contestualmente, anche nel mondo legale – forense, si stono sviluppati, negli ultimi anni, due diverse tipologie di i. a.: i software di assistenza agli avvocati; i software in grado di svolgere attività di decisione e valutazione.

Quanto ai software di assistenza, si pensi alle banche dati che già da tempo si sono diffuse come strumenti di ausilio nelle ricerche giuridiche online all'interno degli studi legali. Eppure, esistono alcune banche dati (cd. di metodo boliano) che in qualche modo appartengono al passato, a cui si stanno affiancando altre di più recente evoluzione.

[19] L'avvento di un giudice *robot* sarebbe certamente utile per assicurare alla giustizia una maggiore celerità ed efficienza nonché per evitare una eccessiva disomogeneità giudizi, ma nel contempo negativo sotto un duplice profilo: da un lato, perché i precedenti giurisprudenziali finirebbero per condizionare i successivi giudizi a ad oggetto le medesime questioni fattuali o giuridiche; dall'altro, perché verrebbe sminuita la valenza persuasiva delle tecniche argomentative, che tradizionalmente possono anche a suscitare empatia nel giudice.

[20] Borruso, *Computer e diritto, Analisi giuridica del computer,* I, Milano, 1988, p. 200.

Altri esempi di software che assistono i legali sono i cd. gestionali, vengono progettati in cloud per comprendere quantità sempre maggiori e tipologie diverse di dati.

Altresì, vi sono altri software più avanzati, in cui si è tentato di sviluppare una attività decisionale del sistema. In Gran Bretagna, è diffuso il Contract review information, un software che offre la correzione automatica dei contratti. L'obiettivo sarà quello di sviluppare un softwre, non solo capace di analizzare i contratti, ma di redigerli come un vero professionista.

Attualmente, esistono anche altri sistemi più evoluti di i. a., in cui il software non si limita più ad eseguire meramente l'attività richiesta ma che sappia elaborare una decisione[21]. Tra gli altri software si citano: A.i. meets legal research[22], che dal 2016 si è diffuso anche in Italia[23]; chatbot[24]; Donotpay[25], considerato il primo robot avvocato che a New York e a Londra ha già contestato, con successo, oltre160.000 multe in soli ventuno mesi di attività; il sistema COIN (acronimo di "Contract intelligence"[26]); infine, il database toga[27].

In questo contesto, potrebbe immediatamente emergere la preoccupazione circa la possibilità che tali professioni verranno completamente sostituite dai software di intelligenza artificiale. A tal proposito si rileva che da uno studio[28], condotto dalla

[21] Numerose imprese stanno integrando il *software* Amelia nelle loro attività operative. Ad esempio: una società internazionale di oil&gas ha istruito Amelia per fornire un riscontro più rapido e efficiente alle richieste dei fornitori in merito alle loro fatture; una banca *leader* a livello europeo ha completato rapidamente l'implementazione di Amelia all'interno della funzione IT; una grande società statunitense di servizi media ha insegnato ad Amelia a dare un supporto di primo livello agli operatori per migliorare il servizio clienti; una banca, attraverso Amelia, ha fornito assistenza sui dettagli delle *policy* interne.

[22] Si tratta di una piattaforma di ricerca legale alimentata da intelligenza artificiale per la legge degli Stati Uniti. Il *software* è in grado di rispondere, con precisione ed in pochi secondi, ai quesiti giuridici formulati *online* dai clienti.

[23] Il *software* è attivo in nove studi legali a Milano e può arrivare a sostituire l'attività di ben sessanta professionisti.

[24] *Chatbot* è un *software* progettato per simulare una conversazione con un essere umano.

[25] Il *software* è stato realizzato da Joshua Browder, inizialmente con l'intento di contestare le multe, che attualmente simula l'attività di un vero e proprio avvocato, esperto in oltre 1000 campi giuridici, per i quali può dare assistenza in tutti gli USA e in UK, in maniera completamente gratuita.

[26] Il sistema automatizzato, utilizzato dalla banca americana "*Jp Morgan Chase and co*" è in grado di leggere ed interpretare accordi commerciali e contratti d finanziamento in tempo reale, semplificando il lavoro dei propri legali.

[27] Un *database* in cui sono state censite tutte le fattispecie criminose disciplinate dal codice penale e dalla legislazione speciale, che permette di verificare: la competenza, la procedibilità, l'ammissibilità alternativi, i termini prescrizionali e di durata delle misure cautelari, nonché di calcolare la pena per ciascun tipo di reato.

[28] Lo studio è stato condotto nell'ambito dell'*Oxford Martin Programme on the Impact of Future Technology*, sul tema dell'impatto della automazione sui lavori esistenti.

Oxford University nel 2013, è emerso che circa la metà delle settecento occupazioni esaminate, sono destinate a scomparire[29]. Eppure, tra le professioni non a rischio di estinzione ritroviamo: insegnanti, medici, artisti e, in genere, coloro i quali svolgono attività richiedono intense interazioni sociali e gli avvocati.

5. Profili etici e deontologici.

In questo contesto emerge l'importanza della nozione: *"the law tell as what we can do, the ethic tell as what we should do".*

Ad oggi, i software, seppure si siano maggiormente evoluti, non sono ancora in grado di prendere autonomamente decisioni che siano coscienti e morali, in quanto non godono della qualità etica della consapevolezza.

Sul tema è intervenuta, il 4 dicembre 2018, la Commissione Europea per l'Efficacia della Giustizia (CEPEJ) del Consiglio d'Europa ha emanato la "Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia e nei relativi ambienti"[30]. Per la prima volta, a livello europeo, si è preso atto della "crescente importanza della intelligenza artificiale (IA) nelle nostre moderne società e dei benefici attesi quando q sarà pienamente utilizzata al servizio della efficienza e qualità della giustizia", e sono state individuate alcune linee guida fondamentali.

In particolare, la Carta etica, nel tentativo di bilanciare l'interesse di un progresso dell'efficienza del sistema giudiziario e la tutela dei diritti fondamentali, enuncia i seguenti principi: 1) principio del rispetto diritti fondamentali; 2) principio di non discriminazione; 3) principio di qualità e sicurezza; 4) principio di trasparenza; 5) principio di garanzia dell'intervento umano. Questo principio è particolarmente rilevante in ambito giudiziario, ove il giudice deve mantenere il potere di verificare l'output intelligente rispetto al caso specifico, per garantire l'effettiva applicazione del diritto al caso specifico. Ogni utente dovrà essere informato della natura della soluzione proposta tramite AI, le possibili opzioni e del diritto di ricorso.

[29] I primi lavori che presto potrebbero essere affidati alle macchine sono quelli di operatori di *call center*, bibliotecari, trascrittori, analisti finanziari, magazzinieri, autisti di taxi, lavoratori edili e cuochi.

[30] Si tratta di uno studio di alcuni esperti che ha proposto - attraverso la Carta etica - un'ipotesi di 'codice deontologico' del robot-giudice.

La Carta etica è indirizzata sia alle start up che progettano piattaforme di nuovi servizi, sia agli sviluppatori di tools, sia alle autorità a cui spetta la decisione di regolare questo campo, nonché ai professionisti del settore giuridico (magistrati, avvocati, notai).

Contestualmente, con riferimento al rapporto tra l'i. a. e l'avvocatura, assume un ruolo pregnante il codice deontologico forense. Attualmente, infatti, l'i. a. non è in grado di prendere autonome decisione che siano morali e soprattutto deontologiche.

A tal proposito, si rileva che, il codice deontologico forense, all'art. 9,[31] sancisce i doveri di indipendenza, lealtà, correttezza, probità, dignità, decoro, diligenza e competenza; all'art. 11[32] ribadisce la libertà dell'avvocato "nell'accettare l'incarico"; all'art. 23, n. 4 sancisce che, al momento del conferimento dell'incarico, l'avvocato non deve consigliare azioni "inutilmente" gravose; all'art. 23, n. 5 precisa, altresì, che l'avvocato deve rifiutare di prestare la propria attività se, dagli elementi conosciuti, desuma che essa sia finalizzata alla realizzazione di operazione illecita.

In conclusione, in un processo di robotizzazione dell'uomo e di umanizzazione del robot, è necessario accentrare la tutela dei diritti fondamentali.

[31] Art. 9 c.d.f.: "*L'avvocato deve esercitare l'attività professionale con indipendenza, lealtà, correttezza, probità, dignità, decoro, diligenza e competenza, tenendo conto del rilievo costituzionale e sociale della difesa, rispettando i principi della corretta e leale concorrenza*".

[32] Art. 11 c.d.f.: "*Rapporto di fiducia e accettazione dell'incarico. 1. L'avvocato è libero di accettare l'incarico*."

La Tutela del Copyright nella Società dell'Informazione.

di Giulio Riccio

Sommario. 1. Premessa. **2.** Internet ed il Web. 3. Il linking ed il framing online. 4. L'attività della Corte di Giustizia dell'Unione europea. 5. Il linking. 6. Il framing. 7. Conclusioni.

Modern society is referenced to as "information society" since it is characterized by cutting-edge technologies able to process data and exchange information rapidly at any time across the world.

This work addresses and deepens the topic of copyright protection in the modern information society.

This topic is significant since it has emerged as the core of the institutional political debate, considering the recent approval of the EU directive n. 2016/280, which will attempt to update the regulatory systems of the EU Member States to the advanced technological scenario.

1. Premessa

I recenti progressi tecnologici hanno avuto un grande impatto sulla vita degli utenti rivoluzionando le modalità di comunicazione tra persone fisiche e giuridiche e contribuendo alla nascita della c.d. "società dell'informazione"[33].

Internet è oggi capace di raggiungere in modo pervasivo dispositivi mobili capaci di elaborare dati e scambiare informazioni in ogni momento da un capo all'altro del globo e ad altissima velocità[34].

Recentemente, è diventato di uso comune il termine "big data" che caratterizza queste enormi quantità di dati ed informazioni e l'insieme dei metodi e delle tecnologie impiegate per analizzarle. I big data rivestono un fondamentale ruolo strategico nella

[33] S. CRAWFORD, *The Origin and Development of a Concept: The Information Society*, 1983, Bull. Med. Libr. Assoc. 71(4) October, 380

[34] M. HARDT, A. NEGRI, *Multitude: War and Democracy in the Age of the Empire*, 2005, New York: Hamish Hamilton, 108

società contemporanea poiché da essi è possibile estrapolare significative indicazioni sugli utenti, individuando relazioni aggiuntive tra fenomeni diversi e tentando di prevedere trend futuri relativamente a scelte e preferenze degli utenti profilati, in modo migliore di quanto si potrebbe fare analizzando separatamente piccole quantità di dati.

Queste informazioni hanno un notevole valore economico e sono, pertanto, estremamente appetibili. I nuovi pericoli per i dati privati degli utenti hanno prodotto un crescente interesse da parte delle istituzioni nazionali e dell'Unione europea che ha posto le basi per assolvere gli obiettivi contenuti nei Trattati[35] nel tentativo di armonizzare le normative degli Stati membri mediante lo strumento delle direttive.

In tale contesto, sono nate nuove sfide per il diritto, chiamato a disciplinare nuovi fenomeni relativi alla privacy, all'identità digitale, all'eredità digitale, alla tutela del copyright delle opere digitali (e/o digitalizzate) nel mondo «virtuale».

Le opere digitali, in particolare, circolano in Rete ad una velocità tale da rendere obsolete le tecniche di tutela tradizionalmente previste. Il legislatore, per far fronte a tale situazione, si è dunque avvalso di strumenti idonei ad affiancare i "classici" rimedi giurisdizionali in una posizione alternativa ad essi, nel duplice obiettivo di offrire al cittadino una rapida risoluzione delle controversie e contribuire, di riflesso, al decongestionamento del carico del contenzioso giudiziale.

Nell'ordinamento giuridico italiano, relativamente alla tutela del copyright online, tali tipi di strumenti sono stati previsti dall'Autorità per le Garanzie nelle Comunicazioni (Agcom) con l'allegato A della Delibera 680/13/CONS, intitolato «Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70»[36].

In virtù di tale Regolamento l'Autorità può, in seguito alla presentazione di un'istanza, adottare "ordini" tesi ad impedire l'accesso a quei siti che illecitamente mettono a disposizione degli utenti opere digitali protette da copyright, oppure può disporre l'archiviazione del procedimento.

Le modalità classiche di condivisione di opere potenzialmente lesive del diritto d'autore in Rete sono il linking ed il framing. Mentre con il linking si permette

[35] Trattato sull'Unione europea (TUE) e Trattato sul Funzionamento dell'Unione europea (TFUE)

[36] Consultabile all'URL https://ddaonline.agcom.it/AllegatoA.html

all'utente di entrare nella home page del sito linkato (surface linking) oppure direttamente nelle sue pagine interne (deep linking), con la tecnica del framing il contenuto del sito linkato appare all'utente all'interno del sito consultato, rendendo difficile operare una distinzione tra i due siti.

Questo lavoro affronta ed approfondisce il tema della tutela del copyright nella moderna società dell'informazione. Tale tema è rilevante poiché è al centro del dibattito politico istituzionale, alla luce della recente approvazione della direttiva Ue n. 2016/280, con cui si tenterà di adeguare i sistemi normativi degli Stati membri al progredito scenario tecnologico.

Il prosieguo dell'articolo è organizzato come segue: in Sezione I è offerta una panoramica sul Web e sulla sua evoluzione. Sezione II descrive come il linking e il framing come elementi di criticità per la tutela del copyright. In Sezione III, è descritto l'attività della Corte di Giustizia dell'Unione europea in tale merito. Infine, Sezione IV trae le conclusioni.

2. **Internet ed il *Web***

Il World Wide Web (o semplicemente *Web*), nato ufficialmente il 6 agosto del 1991, ha rivoluzionato il modo di inviare e ricevere informazioni e può essere considerato la causa della diffusione repentina ed esponenziale del fenomeno telecomunicativo[37].

Il termine *Web* significa letteralmente "ragnatela globale" che costituisce un vero e proprio strumento di informazione. Esso fu concepito dall'informatico inglese Tim Berners-Lee che alla fine degli anni '80 era in cerca di un mezzo di condivisione dei documenti all'interno dei vari uffici del CERN di Ginevra, presso cui lavorava[38].

In poco meno di un decennio questa rete interna alla comunità scientifica è stata resa pubblica ed è diventata un mezzo di informazione e conoscenza che ha integrato e talvolta soppiantato quelli tradizionali, rivoluzionando la storia al pari dell'invenzione della stampa a caratteri mobili[39], della radio e della televisione.

Chiunque disponga di un computer e di un accesso ad Internet, infatti, può accedere a contenuti multimediali che si trovano su dispositivi remoti, oppure può creare

[37] G. CIACCI, G. BUONOMO, *Profili di informatica giuridica*, I ed., Cedam, 2018, 98
[38] *Ibidem*
[39] Introdotta in Europa da Johannes Gutenberg nel 1455, mentre in Asia esisteva fin dal 1041

un sito in cui pubblicizzare la propria attività imprenditoriale, pubblicare i propri traguardi professionali, annotare i propri pensieri, esporre le proprie opere artistiche, ecc., rivolgendosi direttamente e liberamente a tutti gli utenti della Rete.

La naturale evoluzione del *Web* è stata il passaggio da una dimensione "statica" (o *Web 1.0*) in cui vi era la possibilità di collegarsi e visualizzare siti attraverso collegamenti ipertestuali (i c.d. link) al c.d. *Web 2.0*[40]. Ciò attraverso un approccio filosofico alla Rete che ne connota la dimensione sociale e della condivisione, rispetto ad una fruizione di tipo passivo, come in precedenza.

Tale evoluzione permette di accedere a nuove funzionalità, tra cui: fruire, modificare e creare contenuti multimediali, oltre che interagire con altri utenti. Sebbene molti strumenti della Rete possano apparire invariati (come forum, chat e blog, già esistenti negli anni '90), le nuove modalità di utilizzo degli stessi hanno aperto nuovi scenari ed hanno consentito nuove possibilità di collegamento ed interazione tra soggetti distanti nello spazio e nel tempo.

Alle prime virtual communities dedicate a gruppi scientifici o agli studiosi dell'informatica si sono così affiancate quelle rivolte ai più disparati temi, fino all'avvento dei social network, siti Internet che forniscono agli utenti un luogo d'incontro virtuale in cui scambiare dati, messaggi, condividere post, foto e video, chattare, ecc.[41]

Con l'avvento delle communities si sono palesate criticità relative alla tutela dei diritti degli utenti in Rete, tanto pregnanti da animare il dibattito pubblico e da rendere necessaria l'emanazione di importanti provvedimenti da parte delle istituzioni dell'Unione europea[42].

3. **Il linking ed il framing online**

Oggetto di scambio sulla rete possono essere testi, immagini oppure possono essere contenuti di tipo multimediale come nel caso delle c.d. opere digitali[43].

---

[40] T. O'REILLY, *What Is Web 2.0*, O'Reilly Network, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, 2005

[41] Il social network ad oggi più noto è Facebook, lanciato il 4 febbraio 2004 ed originariamente progettato per gli studenti della Harvard University di Cambridge (USA)

[42] Un esempio per tutti è l'emanazione del Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

[43] Si parla di "opere digitali" in presenza di «un'opera, o parti di essa, di carattere sonoro, audiovisivo fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica», ai sensi dell'art. 1, lett. p), Regolamento Agcom.

Proprio la digitalizzazione delle opere ha provocato la crisi del tradizionale sistema di tutela del diritto d'autore e dei diritti connessi, non più idoneo ad essere applicato nel contesto telematico in cui i classici sistemi di controllo tesi a garantire i diritti dell'autore e reprimere i fenomeni di pirateria non sono efficaci.

Agli albori di Internet, quando i siti visitabili erano ancora costituiti da testo e caratteri standard, un efficace modo per la circolazione online di informazioni erano i collegamenti ipertestuali (link) contenuti nelle varie pagine consultabili.

Grazie ad un link, infatti, si può raggiungere direttamente un sito cliccando su una parola attiva (c.d. hotword), nel caso in cui a questa sia collegato un indirizzo Internet (URL, Uniform Resource Locator). I link sono, in pratica, vere e proprie rotte di "indirizzamento" verso URL che altrimenti sarebbe difficilmente raggiungibili[44].

Il linking è una caratteristica primaria del Web, basti pensare che i motori di ricerca quotidianamente utilizzati dagli utenti sono essenzialmente un elenco di link ordinati per contenuto (*e.g.* Google, Bing, DuckDuckGo).

Il link può, quindi, essere considerata una "porta" di accesso ad altri siti e ad altri documenti i quali, a loro volta, possono essere connessi con ulteriori informazioni, riproducendo le diramazioni di una ragnatela di cui non si può prevedere lo sviluppo.

La possibilità di rinviare ad altri siti, caratteristica fondamentale della libertà della Rete, sin da subito si è configurata come potenzialmente lesiva dei diritti dell'autore dei siti a cui si viene reindirizzati, laddove quest'ultimo non presti il proprio consenso al linking.

Anche il c.d. framing (o tecnica dell'inclusione), che consente di linkare ad un sito includendolo nell'interfaccia grafica del sito linkante, può costituire un uso illecito dei contenuti online altrui. Infatti, il sito linkato, posizionandosi all'interno di quello che lo richiama, rende difficile all'utente capire su quale dei due siti l'opera si trovi effettivamente.

Tali operazioni, se condotte senza l'autorizzazione dei titolari del diritto d'autore e dei diritti connessi, possono costituire una violazione del diritto di riproduzione, di distribuzione e diffusione di opere protette da copyright o, comunque, possono generare confusione in ordine alla titolarità delle stesse.

---

[44] AA.VV. (A CURA DI G. CASSANO), *Diritto delle nuove tecnologie informatiche e dell'Intenet*, I ed., Ipsoa, 2002, 936

Su tali aspetti ha avuto modo di pronunciarsi la Corte di giustizia dell'Unione europea, come descritto nella Sezione successiva.

4. L'attività della Corte di Giustizia dell'Unione europea

Le prime pronunce ad opera di autorità giudiziali, sia statunitensi che europee, relative alla tutela del copyright online ed inerenti a fenomeni di linking e/o framing risalgono alla fine degli anni '90[45] ed hanno fornito un contributo alla nascita della direttiva 2001/29/CE del Parlamento Europeo e del Consiglio del 22 maggio 200.

Obiettivo di tale direttiva è stata l'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione all'interno dell'Unione europea, e può essere considerata diretta discendente dei due trattati WIPO di Ginevra del 1996: il WIPO Copyright Treaty ed il WIPO Perfomances and Phonograms Treaty.

Tale provvedimento, tenuto conto dell'incessante e rapido sviluppo della Rete, è risultato fondamentale per fornire agli organi giudiziali strumenti interpretativi adeguati con cui affrontare le questioni giuridiche attinenti agli illeciti commessi online.

I giudici nazionali sono stati sempre più frequentemente chiamati a pronunciarsi su questioni attinenti alla tutela del copyright online e, scontrandosi con i dubbi interpretativi scaturenti anche dal recepimento della suddetta direttiva negli ordinamenti nazionali, si sono rivolti alla Corte di Giustizia dell'Unione europea, organo deputato ad assicurare la corretta applicazione del diritto dell'Unione europea e la sua interpretazione uniforme.

Il linking ed il framing sono, dunque, divenuti oggetto di importanti pronunce giudiziali da parte della Corte che ha definito la portata normativa delle disposizioni contenute nella predetta direttiva.

5. Il linking

a. Il caso «Svensson» (C-466/12)

La controversia comunemente indicata come caso «Svensson» ha visto contrapposti alcuni giornalisti del giornale e sito Göteborgs-Posten e la Retriever Sverige, che gestiva un sito Internet contenente liste di link reindirizzanti ad articoli pubblicati da altri siti Internet (tra cui quello del predetto giornale).

[45] Tra le più importanti si ricordano: District Court di Rotterdam, sent. 22 agosto 2000; Tribunal de Commerce de Paris, sent. 26 dicembre 2000 (caso Kranten.com); U.S. District Court, Central District of California, sent. 10 agosto 2000 (Caso Ticket-Master Online vs Tickets.com)

La questione era inerente alla possibilità che la condotta della Retriever Sverige (pubblicazione di link ad articoli già liberamente accessibili online di cui non deteneva alcun tipo di diritto e senza alcuna preventiva autorizzazione) potesse configurare la fattispecie di comunicazione a pubblico e, quindi, violare i diritti dei giornalisti e/o del giornale, ai sensi dell'art. 3, par. 1 della direttiva 2001/29/CE[46].

Secondo la Corte di giustizia la messa a disposizione in Rete dei link agli articoli del Göteborgs-Posten da parte del sito di Retriever Sverige non costituiva comunicazione a pubblico (e, quindi, non ledeva i diritti d'autore dei ricorrenti) in quanto era un atto di comunicazione rivolto ad un pubblico che non può essere definito come nuovo.

Le opere dei giornalisti erano, infatti, già liberamente accessibili online, non essendo prevista alcuna misura restrittiva per l'accesso e la lettura degli stessi, con la conseguenza che non era necessaria l'autorizzazione da parte dei titolari del diritto d'autore prevista dal citato articolo.

Non trovava rilievo neanche il fatto che l'utente Internet avesse l'impressione che l'opera fosse messa a disposizione dal sito della Retriever Sverige (contenente i link) mentre gli articoli erano in realtà stati pubblicati sul un sito del giornale.

b. Il caso «GS Media» (C-160/15)

La controversia nota come «GS Media» riguardava la società Sanoma che deteneva diritti esclusivi su alcune fotografie di una *soubrette* olandese che, prima di essere pubblicate su una rivista, erano state messe a disposizione online dalla GS Media sul proprio sito "GeenStijl" mediante link reindirizzanti ad un altro sito in cui le foto erano state rese disponibili.

Il nodo interpretativo da sciogliere riguardava se si fosse in presenza di una «comunicazione al pubblico» qualora l'opera fosse già stata pubblicata senza il consenso del titolare del diritto d'autore. A differenza del caso Svensson, le opere fotografiche della Sanoma, società titolare del diritto d'autore sulle stesse, erano state messe a disposizione in rete senza l'autorizzazione e la conoscenza da parte di quest'ultima ed i

[46] Tale articolo è rubricato «Diritto di comunicazione di opere al pubblico, compreso il diritto di mettere a disposizione del pubblico altri materiali protetti» ed al par. 1 recita: «Gli Stati membri riconoscono agli autori il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente»

link forniti dalla GS Media facilitavano il raggiungere l'indirizzo in cui le predette opere erano state caricate.

Per i giudici, innanzitutto, la nozione di comunicazione al pubblico dev'essere intesa in senso ampio e consta degli elementi di "atto di comunicazione" di un'opera e di "comunicazione" di quest'ultima ad un pubblico ed è necessario tenere conto anche di altri criteri tra loro complementari e interdipendenti e di natura non autonoma; tra questi la Corte evidenzia il ruolo imprescindibile dell'utente e il carattere intenzionale del suo intervento.

Rilevante è, inoltre, la nozione di pubblico inteso come numero indeterminato di destinatari potenziali e comprende, peraltro, un numero di persone piuttosto considerevole. Ulteriore elemento considerato dalla Corte è il carattere lucrativo di una comunicazione al pubblico.

Secondo la Corte, tenuto conto della complessità di Internet e della scarsa cognizione delle conseguenze dei propri comportamenti da parte degli utenti, la messa a disposizione di link costituisce una «comunicazione al pubblico» qualora sia accertato che chi agisce è a conoscenza, o è tenuto ad esserlo, del fatto che lo stesso fornisce accesso ad un'opera illegittimamente pubblicata su Internet (ad esempio perché è stato avvertito dai titolari del diritto d'autore).

Medesima conclusione qualora il link consenta agli utenti di eludere misure restrittive adottate dai titolari dell'opera protetta per limitare l'accesso del pubblico ai soli abbonati; la messa a disposizione di siffatto link costituisce in tal caso un intervento voluto senza il quale gli utenti non potrebbero fruire delle opere protette.

Infine, qualora il linking sia effettuato per fini di lucro, è legittimo aspettarsi che colui che agisce realizzi le verifiche necessarie per garantire che l'opera di cui trattasi non sia pubblicata illegittimamente sul sito cui rimandano i link, cosicché deve presumersi che tale attività sia posta in essere con piena cognizione del fatto che l'opera è protetta e che il titolare del diritto d'autore potrebbe non aver autorizzato la pubblicazione su Internet. Anche in siffatte circostanze, e a condizione che tale presunzione relativa di conoscenza non sia confutata, l'atto di collocare un collegamento ipertestuale verso un'opera illegittimamente pubblicata su Internet costituisce una «comunicazione al pubblico».

6. **Il framing**

c. Il caso «BestWater» (C-148/13)

Nell'ordinanza nota come "BestWater" pronunciata nella controversia tra Best-Water International e i Sig.ri Mebes e Potsch, la Corte ha affrontato il framing, cioè l'inserimento di link nei siti gestiti da Mebes e Potsch che, utilizzando la tecnica di «inclusione», permettevano agli utenti di fruire di un filmato esterno ai predetti siti.

La BestWater International, che godeva di diritti esclusivi sul filmato aveva agito in giudizio per far dichiarare il framing una modalità di comunicazione al pubblico.

La Corte risponde negativamente, rifacendosi a quanto dichiarato nella sentenza relativa al caso Svensson, in quanto la fattispecie concreta non ricadeva in quella prevista di comunicazione al pubblico nella misura in cui l'opera non era stata trasmessa ad un pubblico nuovo (al momento dell'autorizzazione alla comunicazione iniziale dell'opera al pubblico erano stati presi in considerazione tutti gli utenti della rete) né comunicato mediante modalità tecniche specifiche, diverse dalla comunicazione originale.

7. Conclusioni

Negli ultimi anni, grazie anche ai progrediti mezzi a disposizione degli utenti, è stato possibile scambiare una quantità sempre maggiore di informazioni ad una velocità altrettanto crescente.

Il linking ed il framing sono state le prime tecniche attraverso cui gli utenti della rete oggi condividono informazioni ed opere digitali a mettere in crisi i tradizionali sistemi di tutela del copyright e lotta alla pirateria.

Tali fattispecie hanno avuto il pregio di permettere a legislatori e giudici di affrontare quel processo ermeneutico da cui sono stati sintetizzati quei criteri che tutt'oggi devono essere tenuti in considerazione dagli utenti e dai titolari del diritto d'autore e dei diritti connessi in Internet.

Come già anticipato, a distanza di quasi vent'anni dall'emanazione della importantissima direttiva 2001/29/CE, il Parlamento Ue ed il Consiglio hanno approvato la direttiva Ue n. 2016/280 sul copyright, tra non poche polemiche.

Il progetto di direttiva ha riguardato varie questioni, che possono essere raggruppate in tre categorie: 1) adeguamento delle eccezioni/limitazioni al diritto d'autore all'ambiente digitale e all'ambiente transfrontaliero; 2) miglioramento delle procedure

di concessione delle licenze per garantire un più ampio accesso ai contenuti; 3) garanzia di buon funzionamento del mercato per il diritto d'autore.

Tralasciando le disposizioni al centro del dibattito politico ed istituzionale contenute nella predetta direttiva, occorre riflettere sul rapporto tra la tecnologia ed il tempismo dell'intervento normativo da parte delle istituzioni europee.

Ciò non tanto perché l'approvazione è avvenuta a poche settimane dalle elezioni europee al termine di due anni di discussioni, ma perché solo un *focus* attento e costante può garantire un'effettiva tutela del copyright su una Rete che muta e si evolve ogni secondo che passa.

Imprescindibile risulta essere l'educazione alla fruizione dei contenuti online da parte delle nuove generazioni di utenti ed un approccio etico e non passivo agli strumenti messi a disposizione dalle nuove tecnologie nell'era digitale.

LE NUOVE FRONTIERE DELL'ACCESSO GENERALIZZATO E I CONFINI DELLA NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI

di Rosanna Celella

SOMMARIO: 1. Il triplo binario in materia di accesso; - 2. Privacy e accesso amministrativo; 3. - Il nuovo accesso generalizzato e le Linee Guida ANAC.

This paper focused on the administrative access discipline provided for by the Italian legislator. In particular, it investigates the relationship between the right of access and the protection of personal data, which rapresents one of the most important limit on the right of access.

1. Il triplo binario in materia di accesso

Il legislatore nazionale ha fortemente inteso rafforzare negli ultimi anni il principio di trasparenza finalizzato ad ampliare il controllo diffuso sull'attività della pubblica amministrazione; in particolare il D.Lgs. del 14 marzo 2013, n. 33 (T.U. sulla trasparenza) ha operato un riordino della disciplina riguardante gli obblighi di trasparenza amministrativa.

Uno degli strumenti per garantire la trasparenza amministrativa è sicuramente il diritto d'accesso ai documenti amministrativi che risponde ad una triplice finalità: assicurare un controllo diffuso sull'attività della pubblica amministrazione (di seguito anche PA), garantire l'obbligatorietà in capo alla PA di agire in regime di totale trasparenza, consentire una partecipazione più consapevole dei cittadini all'operato della PA.

Oggi la disciplina dell'accesso presenta uno sistema a triplo binario[47]: l'accesso procedimentale di cui alla legge 7 agosto 1990, n. 241 (legge sul procedimento amministrativo), l'accesso civico di cui all'art. 5[48] co. 1 del D.Lgs. 33/13 e, da ultimo, l'accesso universale (o generalizzato) di cui al co.2 dello stesso articolo.

[47] F. CARINGELLA, Manuale di diritto amministrativo, Dike, 2017.
[48] Articolo 5 (Accesso civico a dati e documenti)

L'accesso procedimentale previsto dalla l. 241/1990 è un istituto preordinato alla conoscenza di documenti preesistenti e individuati e non può essere utilizzato per formare nuovi documenti o per ottenere informazioni sullo stato di un procedimento amministrativo. Inoltre, l'esercizio del diritto di accesso viene circoscritto alle sole informazioni contenute in documenti amministrativi, con esclusione quindi di quelle che non rivestono la forma di documento (ad eccezione degli enti locali, in cui è previsto l'accesso alle informazioni anche se non ancora tradotte in documenti amministrativi). Si ricorda, tuttavia, che in materia ambientale vige una speciale disciplina diretta a favorire l'accesso e finalizzata a garantire un controllo sociale diffuso sulla qualità dell'ambiente. Inoltre, per poter avvalersi dello strumento dell'accesso procedimentale è necessaria la legittimazione ad agire: l'interessato deve avere un interesse qualificato alla presa visione o estrazione di copie del documento.

L'accesso civico di cui al co.1 dell'art. 5 del D.Lgs. 33/2013, invece, è un diritto che spetta a chiunque: qualsiasi cittadino può esercitare tale diritto, senza il dovere di dimostrare la sussistenza di un interesse specifico e senza la necessità di motivare la richiesta di accesso. Inoltre, questa ipotesi di accesso non riguarda solo i documenti, ma altresì informazioni o dati e anche se non ancora pubblicati dalla PA.

Il nuovo strumento dell'accesso universale di cui al co. 2 invece è ispirato al FOIA (*Freedom of Information Act*) diffuso negli USA e stabilisce per chiunque il diritto di accedere a dati e documenti ulteriori rispetto a quelli oggetto di pubblicazione; si differenzia quindi dall'accesso civico di cui al co. 1 che invece può avere ad oggetto solo dati e documenti che la PA ha comunque l'obbligo di pubblicare. Si precisa tuttavia che, mentre l'accesso civico non richiede il contradditorio tra le parti, in quanto il bilanciamento tra interesse alla pubblicità e interesse alla segretezza è effet-

---

"1. L´obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

2. Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull´utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall´articolo 5-bis".

tuato a monte dal legislatore, l'accesso universale, potendo incontrare limitazioni derivanti dalla necessità di tutelare alcuni diritti fondamentali, richiede il contraddittorio con gli eventuali controinteressati.

È evidente che l'accesso generalizzato non sostituisce l'accesso civico "semplice" previsto dall'art. 5, co. 1 del decreto trasparenza. I due diritti di accesso, pur accomunati dal diffuso riconoscimento in capo a "chiunque", indipendentemente dalla titolarità di una situazione giuridica soggettiva connessa, operano su binari differenti, come si ricava anche dalla clausola di esclusione di cui all'art. 5 co.5, "fatti salvi i casi di pubblicazione obbligatoria". L'accesso generalizzato è autonomo e indipendente da obblighi di pubblicazione e incontra quali unici limiti, da una parte, il rispetto della tutela degli interessi pubblici e/o privati indicati all'art. 5 bis co. 1 e 2, e dall'altra, il rispetto delle norme che prevedono specifiche esclusioni (art. 5 bis, co. 3).

L'accesso generalizzato deve essere anche tenuto distinto dalla disciplina dell'accesso ai documenti amministrativi di cui all'art. 22 e ss. della legge 241/90 (accesso procedimentale), la cui finalità è ben differente da quella sottesa all'accesso generalizzato. L'accesso procedimentale è infatti finalizzato a garantire all'interessato l'esercizio delle proprie facoltà (partecipative e/o oppositive) per la tutela di posizioni giuridiche qualificate. L'interessato difatti deve dimostrare di essere titolare di un "interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso". Vi è di più; mentre la a legge 241/90 esclude l'utilizzo del diritto di accesso finalizzato a sottoporre l'amministrazione a un controllo generalizzato, il diritto di accesso generalizzato ha proprio lo scopo di "favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico". Dunque, l'accesso agli atti di cui alla l. 241/90 e l'accesso civico (generalizzato e non) di cui al D.Lgs 33/13 operano su basi giuridiche e presupposti diversi e tenerli ben distinti è essenziale altresì per calibrare i diversi interessi in gioco e approntare, laddove richiesto, un corretto bilanciamento di interessi caso per caso. Nell'ipotesi di accesso generalizzato, in particolare, le esigenze di controllo diffuso - ma non ben circostanziate - del cittadino consentiranno un accesso meno in profondità (in relazione all'operatività degli eventuali e molteplici limiti), pur essendo tale tipologia di accesso più estesa.

2. Privacy e accesso amministrativo

Un limite che incontra il diritto d'accesso è senz'altro il diritto alla protezione dei dati personali. In tale circostanza, infatti, si contrappongono opposti valori costituzionali: da un lato abbiamo la funzionalità dell'accesso al diritto di difesa in giudizio ex art. 24 Cost. e a garantire l'imparzialità ed efficienza della PA come previsto dall'art. 97 Cost.; dall'altro abbiamo il riconoscimento della riservatezza quale diritto fondamentale della persona e per tanto inquadrato nell'alveo dell'art. 2 Cost. Nello specifico la legge 241/90 configura la riservatezza in due modi: riservatezza delle persone fisiche (art. 2 Cost.) e riservatezza di gruppi, persone giuridiche, enti e associazioni, intesa quindi come riservatezza commerciale o industriale e quindi know how (art. 41 Cost.).

L'art. 24 della l. 241/90, in particolare, prevede che l'accesso ai documenti amministrativi deve essere comunque garantito quando necessario per curare o difendere i propri interessi giuridici. Nel caso in cui però i documenti contengano dati sensibili o giudiziari, l'accesso è garantito nei limiti di quanto previsto dall'art. 60 del Codice privacy, ossia solo previa valutazione comparativa in concreto delle esigenze contrapposte.

Il bilanciamento tra dritto di accesso e diritto alla protezione dei dati personali si effettua oggi tenendo conto del combinato disposto tra la legge 241/90, il D.Lgs 33/13 e il Codice privacy, così come è stato di recente novellato dal D.Lgs 101/2018 che ha realizzato l'adeguamento della normativa nazionale a quella europea (GDPR).

Il capo 1[49] del Codice privacy novellato, rubricato "Accesso ai documenti amministrativi" prevede che per il trattamento dei dati personali in genere, ivi compresi

---

49 Art. 59. Accesso a documenti amministrativi e accesso civico

"1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. 1-bis. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33".

Art. 60 (Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)

"1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale".

le categorie particolari di dati e i dati giudiziari (ex artt. 9 e 10 GDPR) si rimanda alla disciplina di cui alla legge 241/90, così come in caso di accesso civico si rimanda a quanto previsto dal D.Lgs. 33/13.

La legge 241/90 prevede l'ammissibilità dell'accesso anche per le categorie particolari di dati (dati sensibili), ma nella sola forma della visione del documento (senza estrazione di copia). Il trattamento di tali dati, tuttavia, è possibile solo in presenza di un'apposita disposizione di legge che specifichi tipologie di dati, modalità di trattamento e le finalità di rilevante interesse pubblico perseguito. Per i cd. dati sensibilissimi, ossia i dati idonei a rivelare stato di salute o vita sessuale dell'interessato, l'art. 60 del Codice privacy prevede che il diritto di accesso può essere esercitato solo se la situazione giuridica rilevante sottesa allo stesso sia di rango almeno pari al diritto alla protezione dei dati personali (relativi a salute e vita sessuale dell'interessato); pertanto l'accesso sarà giustificato solo se l'interesse sotteso ad esso rientri tra i diritti o libertà fondamentali inviolabili.

Il D.Lgs. 33/13, invece, prevede all'art. 5-bis un elenco di esclusioni e limiti al diritto di accesso e tra questi è annoverata la protezione dei dati personali, in conformità con la disciplina legislativa in materia; la disposizione normativa procede stabilendo che il diritto di accesso è inoltre limitato nei casi in cui risulti subordinato al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all´articolo 24, co.1 della legge 241/90.

In materia di contratti pubblici - e quindi nelle pubbliche gare - il rapporto tra accesso e riservatezza assume particolare rilevanza, in quanto l'interesse di trasparenza della PA nella scelta dei soggetti partecipanti si scontra con l'interesse delle imprese partecipati alla gara di salvaguardare il loro know how industriale. Il Codice dei contratti pubblici ha introdotto doveri di non divulgazione del contento di determinati documenti, nonché limiti oggettivi e soggettivi all'accessibilità degli atti di gara. Il divieto assoluto di non divulgazione concerne la documentazione suscettibile di rivelar il know how industriale e commerciale dell'impresa, onde evitare che i competitor strumentalizzino il diritto d'accesso, utilizzandolo non per verificare la correttezza del provvedimento di aggiudicazione di una gara, ma per sfruttare le conoscenze detenute

da altri e trarne così indebito vantaggio. L'art. 53 del D.Lgs. 50/2016, tuttavia, stabilisce che l'accesso è comunque consentito quando strumentale per l'esercizio di difesa in giudizio, fatti salvi i limiti di cui alla legge 241/90 e al Codice privacy.

In conclusione, la strada da seguire è sempre quella di effettuare un corretto bilanciamento di tutti gli interessi in gioco, nel rispetto delle disposizioni che regolano il procedimento amministrativo, la trasparenza amministrativa e la protezione dei dati personali. Fondamentali, poi, soprattutto in materia di accesso generalizzato, sono le Linee Guida adottate dall'Autorità nazionale anticorruzione (ANAC), d'intesa con il Garante per la protezione dei dati personali, cui sarà dedicata ampia trattazione nel paragrafo successivo.

3. Il nuovo accesso generalizzato e le linee guida ANAC.

Rappresenta ormai un'opinione comunemente diffusa quella di considerare privacy e trasparenza come concetti antitetici: l'esigenza di trasparenza amministrativa si fermerebbe laddove dovessero intervenire esigenze di tutela dei dati personali. Tuttavia tale osservazione non è del tutto corretta, in quanto il principio di trasparenza delle informazioni rappresenta, soprattutto dopo l'entrata in vigore del Regolamento UE 679/2016 (GDPR), un principio generale in materia di protezione dei dati personali. Ad ogni interessato è infatti riconosciuto il diritto di essere informato sul trattamento dei propri dati personali, attraverso l'obbligo d'informativa ex art. 13 del GDPR. Appare dunque evidente che la protezione dei dati personali è una disciplina di "trasparenza ante litteram che ha però un raggio di azione di gran lunga maggiore di quello della "trasparenza amministrativa" in quanto, a differenza di quest'ultima, si applica a qualunque titolare del trattamento pubblico e privato"[50]. Pertanto le due discipline non sono affatto antitetiche, bensì complementari.

La nuova disciplina sulla trasparenza, così come modificata dal D.Lgs 25 maggio 2016, n. 97,con l'introduzione dell'accesso civico generalizzato, aumenta però i rischi di frizione tra privacy e trasparenza. Il nuovo accesso civico riconosce infatti, come più volte ribadito, a chiunque il diritto di accedere a tutti i dati e i documenti detenuti dalle pubbliche amministrazioni e non solo a quelli oggetto di specifici obblighi di pubblicazione.

50 F. MODAFFERI, PRIVACY E TRASPARENZA SONO COMPLEMENTARI MA IL DECRETO FOIA AUMENTA IL RISCHIO DI CONFLITTI, ALTALEX, 30/03/2017.

Se da un lato si favoriscono forme diffuse di controllo sull'operato della PA, dall'altro si aprono le porte di accesso ad un'enorme quantità di dati detenuti negli archivi (elettronici e non) di migliaia di enti. Come abbiamo detto poc'anzi, l'accesso civico è escluso negli specifici casi previsti dall'art. 5-bis, co. 3 del D.Lgs. 33/2013 e può essere rifiutato quando il diniego è necessario per evitare un "pregiudizio concreto" agli interessi, pubblici e privati, indicati all'art. 5-bis, co. 1 e 2, tra i quali è annoverata anche la protezione dei dati personali.

Se si considera che gli atti detenuti dalla pubblica amministrazione contengono quasi sempre anche dati personali - sia di cittadini che di pubblici funzionari- si comprende bene che una delle valutazioni che più la PA (e non solo) sarà chiamata a compiere riguarderà proprio il confronto tra il diritto alla conoscenza del richiedente e il diritto alla protezione dei dati degli eventuali controinteressati.

A supporto in tali non affatto semplici valutazioni intervengono le Linee guida adottate dall'Autorità Nazionale Anticorruzione (ANAC), d'intesa con il Garante per la protezione dei dati personali, sentita la Conferenza unificata Stato Regioni.

L'ambito di applicazione soggettivo dell'accesso generalizzato ricomprende le pubbliche amministrazioni, gli enti pubblici economici, ordini professionali, società in controllo pubblico o in partecipazione pubblica ed altri enti di diritto privato assimilato, limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea. L'intento del legislatore è quello di garantire che la cura concreta di interessi della collettività, anche ove affidati a soggetti esterni all'apparato amministrativo vero e proprio, rispondano comunque a principi di imparzialità, del buon andamento e della trasparenza (si pensi ad esempio ai gestori di pubblici servizi).

Sotto il profilo dell'ambito oggettivo, l'accesso civico generalizzato è esercitabile relativamente "ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione". Tuttavia "l'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti", pertanto non è ammissibile una richiesta meramente esplorativa, né generica, ma deve consentire l'individuazione del dato, del documento o dell'informazione, con riferimento alla loro natura e al loro oggetto. Inoltre una richiesta di accesso per un numero irragionevole e sproporzionato di documenti, che imponga un carico di lavoro tale da inficiare il buon funzionamento dell'amministrazione, può essere rigettata, valutando come preminente, in

questi casi peculiari e restrittivamente interpretati, l'interesse al buon andamento dell'amministrazione.

L'accesso generalizzato è escluso nei casi indicati al co. 3 dell'art. 5 bis, che annovera le seguenti eccezioni assolute: a) segreto di Stato; b) ulteriori casi di divieto di accesso o divulgazione previsti dalla legge.

Al di fuori dei casi di eccezioni assolute, la pubblica amministrazione è tenuta ad operare una valutazione basata su un bilanciamento di interessi in gioco e, dunque , se l'ostensione degli atti possa determinare un pregiudizio concreto e probabile agli interessi indicati dal legislatore ai commi 1 e 2. La pubblica amministrazione, dunque, nella sua valutazione dovrà chiaramente individuare il pregiudizio arrecato a uno degli interessi elencati all'art. 5 bis, co. 1 e dimostrare che si tratti di un pregiudizio concreto, ossia direttamente connesso alla disclosure dell'informazione richiesta e che tale pregiudizio rappresenti un evento altamente probabile, e non soltanto possibile. Il pregiudizio concreto, pertanto, va valutato rispetto al momento e al contesto in cui l'informazione viene resa accessibile.

I limiti (definiti come esclusioni relative o qualificate) al diritto di accesso generalizzato derivanti dalla tutela di interessi pubblici elencati nel nuovo art. 5-bis, co. 1 sono inerenti a: a) la sicurezza pubblica e l'ordine pubblico; b) la sicurezza nazionale; c) la difesa e le questioni militari; d) le relazioni internazionali; e) la politica e la stabilità finanziaria ed economica dello Stato; f) la conduzione di indagini sui reati e il loro perseguimento; g) il regolare svolgimento di attività ispettive. I limiti (esclusioni relative o qualificate) al diritto di accesso generalizzato derivanti dalla tutela di interessi privati, previsti all'art. 5-bis, co. 2 sono invece: a) protezione dei dati personali; b) libertà e segretezza della corrispondenza; c) interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali.

L'art. 5-bis, co. 2, lett. a) prevede che l'accesso generalizzato deve essere rifiutato laddove possa recare un pregiudizio concreto «alla protezione dei dati personali, in conformità con la disciplina legislativa in materia». Dunque, con riferimento alle istanze di accesso generalizzato aventi a oggetto dati e documenti relativi a (o contenenti) dati personali, l'ente destinatario dell'istanza deve valutare se la conoscenza da parte di chiunque del dato personale richiesto arreca (o possa arrecare) un pregiudizio concreto alla protezione dei dati personali, in conformità alla disciplina legislativa in

materia; la sussistenza di tale pregiudizio comporta il rigetto dell'istanza, a meno che non si consideri di poterla accogliere, oscurando i dati personali eventualmente presenti, compresi quelli che possono consentire l'identificazione, anche indiretta, del soggetto interessato. In tale contesto, devono essere tenute in considerazione le motivazioni addotte dal soggetto controinteressato. Infatti, laddove la richiesta di accesso generalizzato possa incidere su interessi connessi alla protezione dei dati personali (ma anche alla libertà e segretezza della corrispondenza oppure agli interessi economici e commerciali, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali), l'ente destinatario della richiesta di accesso deve darne comunicazione ai soggetti titolari di tali interessi.

Il richiamo espresso alla disciplina legislativa sulla protezione dei dati personali comporta, quindi, che nella valutazione del pregiudizio concreto, si faccia, altresì, riferimento ai principi generali sul trattamento e, in particolare, al principio di minimizzazione, vlae a dire rendere disponibili e ostentabili i soli dati personali necessari e pertinenti, oscurando il resto.

I limiti operano, infatti, in relazione alla natura del dato, del documento o dell'informazione di cui si chiede l'accesso (art. 5-bis co. 5), oltre che al contesto temporale. L'amministrazione, pertanto, dovrà consentire l'accesso parziale utilizzando, ove possibile e necessario, la tecnica dell'oscuramento di alcuni dati, al fine di proteggere l'interesse confliggente.

Nelle Linee Guida ANAC è altresì specificato che, ai fini della valutazione del "pregiudizio concreto" - che può legittimare il diniego alla richiesta di accesso -, vanno considerate "le conseguenze, anche legate alla sfera morale, relazionale e sociale, che potrebbero derivare all'interessato (o ad altre persone alle quali esso è legato da un vincolo affettivo) dalla conoscibilità, da parte di chiunque, del dato o del documento richiesto. Tali conseguenze potrebbero riguardare, ad esempio, future azioni da parte di terzi nei confronti dell'interessato, o situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo, oppure altri svantaggi personali e/o sociali".

Ad esempio potrà essere oggetto di valutazione l'eventualità che l'interessato possa essere esposto a minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate, come conseguenza dell'avvenuta conoscenza di determinati dati; oppure vanno considerati i

casi in cui la conoscibilità di determinati dati personali da parte di chiunque possa favorire furti di identità o creazione di identità fittizie a scopo fraudolento; ancora, sono da valutare le ragionevoli aspettative di dell'interessato riguardo al trattamento dei propri dati personali al momento in cui questi sono stati raccolti e quindi se determinate conseguenze non erano prevedibili al momento della raccolta dei dati.

L'ente destinatario della richiesta di accesso generalizzato deve far riferimento a diversi parametri nel valutare l'eventuale lesione di interessi inerenti la protezione dei dati personali, tra cui, anche la natura dei dati personali oggetto della richiesta di accesso, nonché il ruolo ricoperto nella vita pubblica, la funzione pubblica esercitata o l'attività di pubblico interesse svolta dalla persona cui si riferiscono i predetti dati. Riguardo al primo profilo, la presenza di particolari categorie di dati (non solo i dati comunemente definiti "sensibili", ma anche dati genetici, biometrici, di profilazione, sulla localizzazione o sulla solvibilità economica) o di dati giudiziari può rappresentare un indicatore di sussistenza di un pregiudizio, laddove la conoscenza da parte di chiunque di tali dati possa essere fonte di discriminazione o di altri tipi di rischi specifici per i diritti e le libertà fondamentali degli interessati. Infine merita rilievo evidenziare anche la circostanza che la richiesta di accesso generalizzato riguardi dati o documenti contenenti dati personali di soggetti minori o di altre fasce deboli e che pertanto può rappresentare un ulteriore indice di esistenza di un pregiudizio.

È evidente che la protezione dei dati personali rappresenta un tema trasversale e di particolare impatto alla disciplina dell'accesso, ma non di certo un limite inteso come un freno alla sua piena e regolare attuazione. Un fattore invece che potrà essere realmente inibitorio è dato invece dall'assetto organizzativo generale della pubblica amministrazione che probabilmente si mostra non ancora pronto ed efficiente a garantire uno strumento di una natura così ampia e innovativa come l'accesso generalizzato. La nostra PA è ancora alle prime fasi del suo processo di digitalizzazione e sicuramente per garantire un riscontro sollecito e produttivo alle eventuali richieste di accesso generalizzato saranno richieste le competenze, gli strumenti e la struttura di una PA digitale, dotata di sistemi di ricerca, archiviazione, gestione e digitalizzazione documentali avanzati e di tecniche e misure di protezione dei dati personali (come tecniche di data masking e oscuramento parziale dei dati) di cui allo stato dell'arte sembriamo essere ancora sprovvisti o comunque non disporne in modo diffuso.

MACHINE LEARNING E GIUSTIZIA PENALE

di Rita Di Marco

SOMMARIO: 1. Premessa 2. La Carta etica europea per l'uso dell'intelligenza artificiale 3. Il machine learning 3 a). L'analisi di documenti e la predisposizione di atti 3.b). La previsione dell'esito di una causa 3 c). La formulazione di giudizi

Machine learning is a method of data analysis that automates the construction of analytical models. It is a branch of Artificial Intelligence and is based on the idea that systems can learn from data, identify patterns independently and make decisions with minimal human intervention. Machine learning technology can facilitate the work of legal practitioners and therefore make justice more efficient, in three different ways. Depending on the type of input given to the system, that is to say the different typology of the data entered, the learning algorithms used by the system and the output, (ie the final result of the processing procedure), in fact , the technology described above can be used to: 1) analyze documents and prepare documents; 2) the prediction of the outcome of a case; 3) the formulation of judgments, even if under human control.

1. Premessa

L'Intelligenza Artificiale è la capacità di un sistema tecnologico di risolvere problemi, svolgere compiti o attività tipici della mente e dell'agire umano[51]. Il machine learning è un metodo di analisi dati che automatizza la costruzione di modelli analitici. È una branca dell'Intelligenza Artificiale e si basa sull'idea che i sistemi possono imparare dai dati, identificare modelli autonomamente e prendere decisioni con un intervento umano ridotto al minimo[52].

2. La Carta etica europea per l'uso dell'intelligenza artificiale.

[1] N. BOLDRINI, *Cos'è l'Intelligenza Artificiale, perché tutti ne parlano e quali sono gli ambiti applicativi*, in http://AI4Business// 01.03.2019

[52] P. MELLO, *Intelligenza artificiale*, in *http://disf.org/intelligenza-artificiale (Documentazione Interdisciplinare di Scienza & Fede)*, 2002

Il 4 dicembre 2018 la Commissione Europea per l'Efficacia della Giustizia (CEPEJ) del Consiglio d'Europa ha emanato la "Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti", in cui attesa la "*crescente importanza della intelligenza artificiale (IA) nelle nostre moderne società e dei benefici attesi quando questa sarà pienamente utilizzata al servizio della efficienza e qualità della giustizia*", vengono individuati alcuni principi, a cui dovranno attenersi "*i soggetti pubblici e privati responsabili del progetto e sviluppo degli strumenti e dei servizi della IA*".

Tali principi sono: 1) principio del rispetto dei diritti fondamentali; 2) principio di non discriminazione; 3) principio di qualità e sicurezza; 4) principio di trasparenza; 5) principio di garanzia dell'intervento umano[53].

L'obiettivo di quest'ultimo, in particolare, è di "*precludere un approccio deterministico*" e ad "*assicurare che gli utilizzatori agiscano come soggetti informati ed esercitino il controllo delle scelte effettuate*".

3. Il machine learning.

Quanto appena affermato implica un'ampia possibilità di utilizzo della IA nell'ambito della giustizia penale, purchè, ovviamente, gli operatori siano soggetti qualificati all'uso del sistema di IA e ogni decisione sia sottoposta, di conseguenza, al controllo umano.

Le due condizioni poc'anzi indicate sono finalizzate ad evitare il rischio di un cd. "approccio deterministico", vale a dire di un eccessivo automatismo o standardizzazione delle decisioni.

In tale ottica, la tecnologia del machine learning può agevolare il lavoro degli operatori del diritto e rendere, pertanto, più efficiente la giustizia, in tre modi diversi. A seconda del tipo di input dato al sistema, degli algoritmi di apprendimento utilizzati dal sistema e dell'output (ossia del risultato finale del procedimento di elaborazione), infatti, la tecnologia sopra descritta può essere adoperata per: a) l'analisi di documenti e la predisposizione di atti; b) la previsione dell'esito di una causa; c) la formulazione di giudizi, seppure sotto il controllo umano.

[53] QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.eu*, 18.12.2018.

a). L'analisi e la predisposizione automatica di atti e documenti.

L'utilizzo della prima modalità in ambito penale potrebbe avvenire nel caso in cui occorra analizzare una copiosa quantità di documenti. Un recente esempio di applicazione dell'intelligenza artificiale in tale campo è quello del sistema "Toga", ossia di un database nel quale sono censite tutte le fattispecie criminose disciplinate dal codice penale e dalla legislazione speciale, che permette di verificare, tra l'altro, la competenza, la procedibilità, l'ammissibilità a riti alternativi, i termini prescrizionali e di durata delle misure cautelari, di calcolare la pena per ciascun tipo di reato [54]

Un altro esempio interessantissimo di applicazione dell'IA si è avuto nel caso dell'indagine relativa al crollo del ponte Morandi, nell'ambito della quale la Procura di Genova ha deciso di utilizzare un software dell'FBI, dotato di algoritmi particolarmente complessi, al fine di incrociare tutti i dati raccolti (corrispondenti a circa 60 terabyte) con quelli dei dispositivi elettronici sequestrati, con la documentazione tecnica ed i pareri dei consulenti sia del P.M. che della difesa[55].

b) La previsione dell'esito di una causa.

La giustizia cd. "predittiva" consiste nella capacità di elaborare previsioni mediante un calcolo probabilistico effettuato da algoritmi operanti su base semplicemente statistica o anche su base logica.

Tale capacità, a seconda della tipologia di dati introdotti nell'elaboratore, può essere utilizzata nel perseguimento di tre differenti obiettivi.

In primo luogo, al fine di prevenire la criminalità: inserendo, infatti, in un computer una serie di dati ricavati da denunce presentate alla Polizia, il sistema è in grado di prevedere luoghi e orari in cui verosimilmente potrebbero essere commessi altri reati della stessa specie[56].

Il secondo fine perseguibile attraverso tale modalità di utilizzo è il reperimento di uno strumento integrativo dell'attività del giurista per l'interpretazione delle norme di diritto necessarie[57].

---

[54] Cfr. C. MORELLI, *Processo penale: operativa la prima applicazione di intelligenza artificiale?* in *www.altalex.com*, 18 giugno 2018.

[55] *L'Italia userà un software dell'FBI per il caso "Ponte Morandi"*, in *http://quifinanza.it*, 4 novembre 2018

[56] M. IASELLI, ***X-LAW: la polizia predittiva è realtà***, in *www.altalex.com*, 28 novembre 2018

[57] L. VIOLA, *Interpretazione della legge con modelli matematici*, Diritto Avanzato, Milano, 2017

In ultimo, tale funzione, mediante il meccanismo sopra illustrato, potrebbe essere applicata con l'obiettivo di "prevedere" l'esito di un giudizio.

c). La formulazione dei giudizi.

In ossequio a quanto stabilito dalla Carta etica europea, si pone a questo punto il problema di comprendere se un machine learning, munito di rete neurale artificiale capace di immagazzinare quantità teoricamente illimitate di dati, quali disposizioni di legge e precedenti giurisprudenziali, dopo un adeguato periodo di apprendimento, possa emettere un giudizio nell'ambito di un processo penale[58].

Nell'ambito della giustizia penale il problema è veramente delicato, in quanto, innanzitutto, il mezzo di prova più frequentemente usato per l'accertamento di fatti materiali è la testimonianza ed una "*macchina"* potrebbe incontrare serie difficoltà nel giudicare se un teste abbia detto o meno la verità. In secondo luogo perché sono veramente molti i criteri di valutazione della prova per cui, specialmente in un processo indiziario, ancor più difficile sarebbe per un elaboratore stabilire se determinati indizi siano da considerarsi gravi, precisi e concordanti per cui da essi possa essere desunta l'esistenza di un fatto.

Il dibattito, dunque, attualmente verte sulla possibilità che una macchina sia o meno in grado di distinguere il vero dal falso, tenendo conto sia di parametri prefissati che dell'esperienza acquisita. Ciò appare possibile in alcune ipotesi. Nel caso di prova testimoniale, ad esempio, si ritiene massima di comune esperienza che un teste di accusa sia credibile se, non avendo rapporti di interesse né motivi di inimicizia con l'imputato, ha riferito i fatti senza contraddizioni intrinseche né difformità rispetto al contenuto di precedenti deposizioni. Un elaboratore opportunamente programmato potrebbe, in base a tanto, effettuare tale valutazione.

Come noto, si può ritenere che il procedimento decisionale consista nella trasformazione di una situazione antecedente indeterminata in una situazione finale determinata, attraverso una serie di sistemazioni parziali intermedie. L'algoritmo, a sua volta, può essere definito come un procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, ovvero non ulteriormente scomponibili, chiari e non ambigui, in un tempo ragionevole. Si tratta, dunque, di un procedimento in cui la rappresentazione grafica delle operazioni da compiere per eseguirlo,

[58] P. BENANTI, *Le macchine sapienti*, Marietti, Bologna, 2018

presenta evidenti affinità con quello di tipo decisionale. In virtù di quanto detto, è possibile, quindi, che un sistema di IA applicato ad un processo penale possa agevolare il giudice nella decisione.

Al momento, dunque, la questione se sia possibile o meno che un robot sostituisca un giudice è discussa. Ed invero, il diritto di ogni persona ad un tribunale indipendente ed imparziale sancito ex art. 6, comma 1, CEDU davanti ad un giudice terzo e imparziale, come stabilito dall'art. 111, secondo comma, Cost., esclude tale possibilità. A sua volta la Carta etica europea del 2018 ammette l'uso dell'intelligenza artificiale nei sistemi di giustizia penale solo sotto il controllo umano. In buona sostanza, dunque, ad un computer potrebbe essere demandata una funzione *ad adiuvandum* del giudice, quale, ad esempio, la soluzione di specifiche questioni costituenti presupposto della decisione da emettere, come accade nel caso di processi di natura tecnica, in cui occorra valutare se il risultato di una determinata prova scientifica sia o meno corretto.

IL CYBERSECURITY ACT SARÀ PRESTO LO SCUDO EUROPEO A DIFESA DI RISCHI E MINACCE INFORMATICI SEMPRE PIÙ INSIDIOSI E SOFISTICATI, CHE RICHIEDONO REGOLE GLOBALI.

di Sergio Guida

SOMMARIO. 1. Introduzione. - 2. Il Global risk report del World Economic Forum. - 3. Il Nono Studio Annuale sui Costi del Cybercrimine di Accenture. – 4. Il Rapporto Clusit 2019 sulla Sicurezza ICT in Italia. – 5. Il Cybersecurity Act . – 6. Considerazioni finali.

International and national organizations, both public and private, continue to churn out data on the increasing complexity and danger of cyber threats, which are now present in all aspects of citizens' lives. The Cybersecurity Act will soon be Europe's regulatory shield in defense of increasingly insidious and sophisticated cyber risks and threats. And that more than ever require global answers. Cybersecurity Act will soon finalize the legal form of regulation and will define new scenarios in the legislation concerning digital security. In addition to establishing the role of the ENISA agency, the regulation will identify the parameters for defining a European level security certification. Article 51 is emblematic for this purpose.

1. Introduzione.

Prestigiose organizzazioni internazionali e nazionali, sia pubbliche che private, continuano a evidenziare la crescente complessità e il pericolo delle minacce informatiche, che sono ora presenti in tutti gli aspetti della vita dei cittadini e richiedono più che mai risposte globali. Il Cybersecurity Act, lo scudo normativo europeo in difesa delle minacce informatiche, sta giungendo al termine del suo iter costitutivo e definirà nuovi scenari nella legislazione in materia di sicurezza digitale. Oltre a specificare il ruolo dell'agenzia ENISA, il regolamento identificherà i parametri per la definizione di una certificazione di sicurezza a livello europeo.

2. Il Global risk report del World Economic Forum.

Nell'edizione 2019 del Global risk report del *World Economic Forum*[59], fra i primi dieci rischi, trovano spazio la sicurezza informatica, gli attacchi su larga scala e il furto di dati. La grande maggioranza degli intervistati prevedeva un aumento dei rischi legati a cyber-attacchi con furto di denaro e dati (82%) e interruzione delle operazioni (80%). Circa due terzi invece si aspettavano problemi per quanto riguarda i rischi legati alla diffusione di fake news e furto d'identità[60].

La capacità del mondo di promuovere l'azione collettiva di fronte a una crescente serie di gravi sfide è entrata in crisi con il peggioramento delle relazioni internazionali e un rallentamento delle prospettive economiche, causato anche da tensioni geopolitiche; tutto ciò contribuisce a ridurre ulteriormente il potenziale di cooperazione internazionale nel 2019[61]. Cinque aree di interesse venivano evidenziate nella *Global Risks Perception Survey* (GRPS: (1) vulnerabilità economiche, (2) tensioni geopolitiche, (3) tensioni sociali e politiche (4) fragilità ambientali e (5) instabilità tecnologiche.

I rischi informatici intensificano il balzo in avanti che hanno registrato nel 2018: quello di "frode e furto massivo di dati" è stato classificato come il rischio numero quattro in termini di probabilità su un orizzonte di 10 anni, con "attacchi informatici" al numero cinque. Ciò conferma uno schema registrato lo scorso anno, con i cyber-rischi che consolidano la loro posizione accanto ai rischi ambientali nel quadrante ad alta probabilità e alto impatto del panorama globale dei rischi[62].

Attacchi informatici "maliziosi" e negligenze nei protocolli di cyber-sicurezza hanno portato a violazioni massive delle informazioni personali nel 2018. Il più grande è stato in India, dove il database governativo *Aadhaar*, il più grande sistema biometrico del mondo con 1,1 miliardi di cittadini registrati, ha subito violazioni multiple che potenzialmente hanno compromesso i record di tutti gli utenti registrati. Altrove, violazioni dei dati personali colpivano circa 150 milioni di utenti dell'applicazione *MyFitnessPal*, e circa 50 milioni di utenti di *Facebook*[63].

---

[59] World Economic Forum, *The Global Risks Report 2019,* Weforum.org, 15/01/2019.

[60] L. FERRO, *Dal climate change alla cybersicurezza: i pericoli del futuro secondo il World Economic Forum*, Innovationpost.it, Politiche e tecnologie per l'industria, 18/01/2019, pag.1.

[61] S. GUIDA, *Rischi e "instabilità" tecnologici nell'edizione 2019 del Global Risks Report del World Economic Forum, Parte 1*, ICT Security Magazine, 29/01/2019, pag.1.

[62] Ibidem, pag.2.

[63] L. FERRO, *Dal climate change alla cybersicurezza: i pericoli del futuro secondo il World Economic Forum*, Innovationpost.it, Politiche e tecnologie per l'industria, 18/01/2019, pag.1.

Nel 2018 abbiamo avuto dimostrazioni di come gli attacchi informatici possano mettere a rischio addirittura delle infrastrutture critiche. Ad esempio, a luglio, alcuni hacker erano riusciti ad ottenere l'accesso alle sale di controllo di alcune aziende di servizi pubblici. La potenziale vulnerabilità delle infrastrutture tecnologiche critiche è diventata sempre più un problema di sicurezza nazionale, tanto che la seconda interconnessione di rischi più frequentemente citata nel GPRS 2019 è l'associazione di cyber-attacchi con l'eventuale sabotaggio di infrastrutture informatiche critiche[64].

3. Il Nono Studio Annuale sui Costi del Cybercrimine di Accenture.

Nel nono studio annuale sui costi dei crimini informatici[65], Accenture e Ponemon Institute analizzano gli scenari attuali per aiutare i leader a indirizzare meglio gli investimenti e le risorse per la sicurezza. Punti principali:

• gli attacchi informatici si stanno evolvendo dal punto di vista di ciò che prendono di mira, dal modo in cui influiscono sulle organizzazioni e dai metodi di attacco che cambiano.

• Si evidenzia il costo crescente del crimine informatico così come le tendenze delle attività dannose.

• Comprendendo dove possono ottenere valore nei loro sforzi di sicurezza informatica, i leader possono minimizzare le conseguenze riducendo il costo del crimine informatico e persino prevenire gli attacchi futuri.

In un panorama digitale in continua evoluzione, è fondamentale tenere il passo con l'impatto delle tendenze informatiche. Secondo lo studio, gli attacchi informatici stanno cambiando per vari motivi, di seguito elencati.

• Obiettivi in evoluzione: il furto di informazioni è la conseguenza più immediata e più rapida del crimine informatico. Ma i dati non sono l'unico obiettivo. I sistemi centrali, come i controlli industriali, vengono violati in una pericolosa tendenza a bloccare e distruggere.

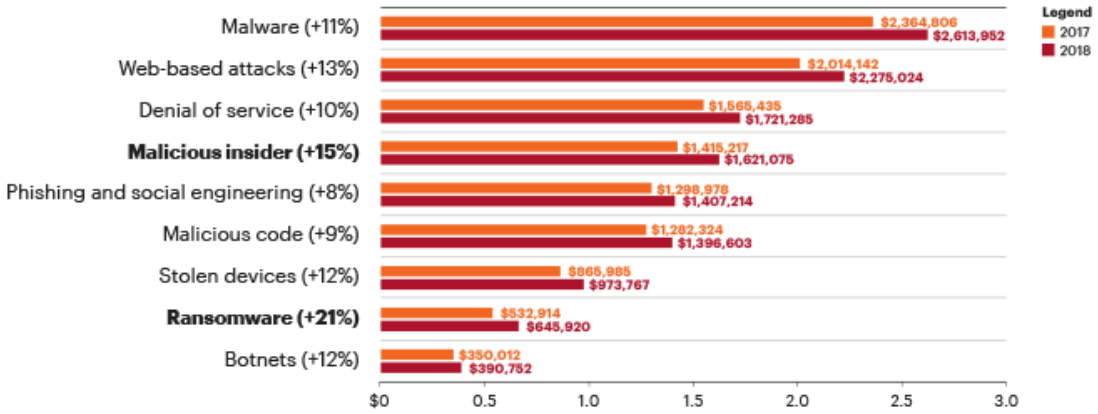
[64] S. GUIDA, *Rischi e "instabilità" tecnologici nell'edizione 2019 del Global Risks Report del World Economic Forum, Parte 1*, ICT Security Magazine, 29/01/2019, pag.3.

[65] Accenture Security, *Ninth Annual Cost of Cybercrime Study. Unlocking the value of improved cybersecurity protection,* Accenture.com, Cyber Resilient Business, 06/03/2019.

• Impatto in evoluzione: mentre i dati rimangono un bersaglio, il furto non è sempre il risultato. Una nuova ondata di attacchi informatici vede i dati non più semplicemente copiati, ma distrutti, o addirittura modificati nel tentativo di generare sfiducia. Attaccare l'integrità dei dati, o favorire la tossicità dei dati, è la prossima frontiera.

• Tecniche in evoluzione: i criminali informatici stanno adattando i loro metodi di attacco. Stanno prendendo di mira lo strato umano - l'anello più debole nella difesa informatica - attraverso l'aumento dei ransomware e degli attacchi di phishing e social engineering come via di accesso. Uno sviluppo interessante è quando stati e/o loro gruppi di attacco associati utilizzano questi tipi di tecniche per attaccare le imprese commerciali. Si tenta di classificare gli attacchi da queste fonti come "atti di guerra" nel tentativo di limitare eventuali coperture assicurative sulla sicurezza informatica[66].

Gli attacchi basati sulle persone sono aumentati maggiormente, come si evince dal grafico seguente:



Lo studio Accenture/Ponemon ha combinato la ricerca in 11 paesi in 16 settori, nei quali sono stati intervistati 2.647 dirigenti senior di 355 aziende, e ha rilevato che la criminalità informatica è in aumento, richiede più tempo per essere risolta ed è più costosa per le organizzazioni. Ma anche che, migliorando la protezione della sicurezza, i costi della criminalità informatica possono essere ridotti e nuove opportunità di guadagno realizzate. I risultati mostrano che:

[66] Accenture Security, *Ninth Annual Cost of Cybercrime Study. Unlocking the value of improved cybersecurity protection*, Accenture.com, Cyber Resilient Business, 06/03/2019, pag.6.

• l’espansione del panorama delle minacce e la nuova innovazione del business stanno portando a un aumento degli attacchi informatici; il numero medio di violazioni della sicurezza nell'ultimo anno è cresciuto dell'11%, da 130 a 145.

• Le organizzazioni spendono più che mai ad affrontare i costi e le conseguenze di attacchi più sofisticati; il costo medio del crimine informatico per un'organizzazione è aumentato di$ 1,4 milioni a $ 13,0 milioni.

• Migliorare la protezione della sicurezza può ridurre il costo del crimine informatico e aprire nuove opportunità di guadagno; è stato calcolato un valore totale a rischio di $ 5,2 trilioni di dollari a livello globale nei prossimi cinque anni.

• Assegnando le priorità alle tecnologie che migliorano la protezione della sicurezza, le organizzazioni possono ridurre le conseguenze della criminalità informatica e sbloccare il valore economico futuro, poiché livelli più elevati di fiducia incoraggiano lo sviluppo delle transazioni.

Per sbloccare il valore della sicurezza informatica sono tipizzabili 3 passaggi:

1. dare priorità alla protezione degli attacchi basati sulle persone; contrastare le minacce interne è una delle più grandi sfide, considerato l’aumento degli attacchi di phishing e ransomware, così come dei malintenzionati. Ad esempio, i Trojan per il mobile banking si attestano tra i malware più flessibili, pericolosi e con il tasso di evoluzione più rapido: con l’obiettivo principale di rubare il denaro dagli account degli utenti, il malware si presenta come un’applicazione legittima e nel momento in cui una vittima accede all’*app* bancaria che crede autentica, i criminali ottengono le credenziali di accesso all’applicazione[67]. Nel primo trimestre del 2019, sono state rilevate circa 30.000 variazioni nella famiglia dei banking Trojan, che hanno tentato di attaccare 312.235 utenti unici, sicché è anche aumentata la loro percentuale nel panorama generale delle cyberminacce (nell’ultimo trimestre del 2018, i banking Trojan per mobile rappresentato l’1,85% di tutti i malware per mobile mentre nei primi tre mesi del 2019 hanno raggiunto il 3,24%[68]);

[67] P. LICATA, *Mobile banking, allarme sicurezza: boom dei trojan cattura-credenziali*, Corriere comunicazioni.it, Cyber Security, 24/05/2019, pag.1.
[68] Ibidem, pag.1.

2. investire per limitare la perdita di informazioni e l'interruzione dell'attività: era già la conseguenza più costosa degli attacchi informatici, ora è una preoccupazione crescente per le nuove norme sulla privacy come GDPR[69] e CCPA[70];

3. mirare a tecnologie che riducono i costi crescenti: utilizzare l'automazione, l'analisi avanzata e la *security intelligence* per gestire l'aumento dei costi di scoperta degli attacchi.

4. Il Rapporto Clusit 2019 sulla Sicurezza ICT in Italia.

Il 2018 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo, ma anche e soprattutto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza. È il quadro che emerge dalla quattordicesima edizione del Rapporto sulla sicurezza Ict del Clusit[71], l'Associazione Italiana per la Sicurezza Informatica.

A livello mondiale, negli ultimi 12 mesi, i Cyber-attacchi gravi censiti sono aumentati del 38% (1.552 contro i 1.127 del 2017), per una media di 129 attacchi gravi al mese, rispetto ai 94 dell'anno prima[72]. Nell'ultimo biennio il loro tasso di crescita è aumentato di 10 volte rispetto al biennio precedente[73].

I settori di attività e le categorie più colpite sono stati *Multiple Targets* (304 attacchi gravi, +37% rispetto al 2017), *Government* (252 attacchi, +41%) e *Healthcare* (159 attacchi, in pratica raddoppiati, +99%). Seguite dal settore bancario e finanziario(+33%), con un forte incremento anche per *Online Services* e *Cloud* (+36%).

Come si vede nel grafico[74], è balzata anche la crescita degli attacchi verso le categorie Fornitori Software e Hardware (+60% in un anno), Grande Distribuzione Organizzata/Retail (+62%).

---

[69] Parlamento Europeo e Consiglio, *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 Regolamento Generale sulla Protezione dei Dati)* ("GDPR"), 27/04/2016.

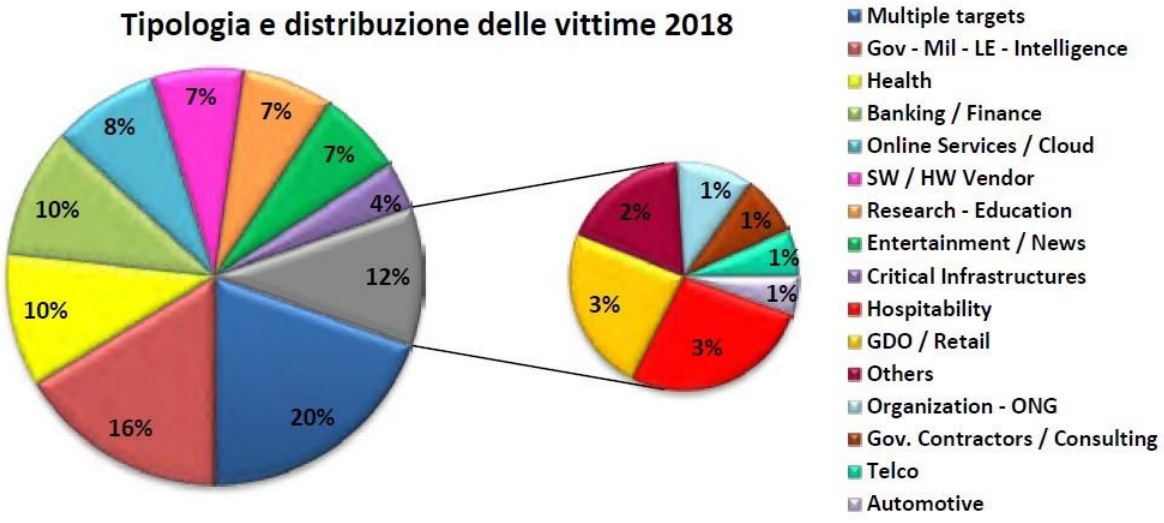
[70] Assembly Bill 375, *The California Consumer Privacy Act of 2018* ("CCPA"), 28/06/2018.

[71] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, pag.12.

[72] D. MANISCALCO, *Cyber, Rapporto Clusit: "Nel 2018 aumentati attacchi gravi". Analizzata la situazione italiana sulla base di oltre 40 milioni di eventi* in OFCS. Report - Osservatorio-Focus per la Cultura della Sicurezza, 13/03/2019.

[73] S. CASINI, *Cyber-security: attacchi in forte aumento ed è allarme anche per l'intelligenza artificiale*, Innovationpost.it, Politiche e tecnologie per l'industria, 21/02/2019, pag.1.

[74] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, pag.27.



Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

È stato ancora il *Malware* 'semplice', prodotto industrialmente, il principale veicolo di intrusione nei sistemi, in crescita del 31% in un anno. Aumentano, invece, del 57% gli attacchi con tecniche di *Phishing* e *Social Engineering* su larga scala, ancora a conferma della logica sempre più 'industriale' dei cyber-criminali.

In uno scenario sempre più a rischio, ad aumentare le preoccupazioni per le prospettive della Cybersecurity sono anche le nuove frontiere dell'Intelligenza Artificiale e del *Machine Learning*: da una parte, tecniche di *Machine Learning* sono utilizzate dai cyber-criminali per compiere attacchi in maniera molto efficace e sempre meno costosa; dall'altra, questi sistemi risultano oggi ancora piuttosto vulnerabili, e quindi facilmente attaccabili, compromessi con tecniche tradizionali o anche attraverso tecniche di *Adversarial machine learning*.

In realtà anche l'importantissima iniziativa della Commissione Europea per lo sviluppo di una 'Trustworthy AI" non pone la Cyber-security tra i requisiti essenziali, tant'è che "nel documento 'Ethics Guidelines for Trustworthy AI"[75] si parla solo di 'Respect for Privacy' e, all'interno del requisito di *'robustness'* dei sistemi, si parla di 'resilience to attack', criteri che di per sé non coprono tutti gli aspetti di sicurezza

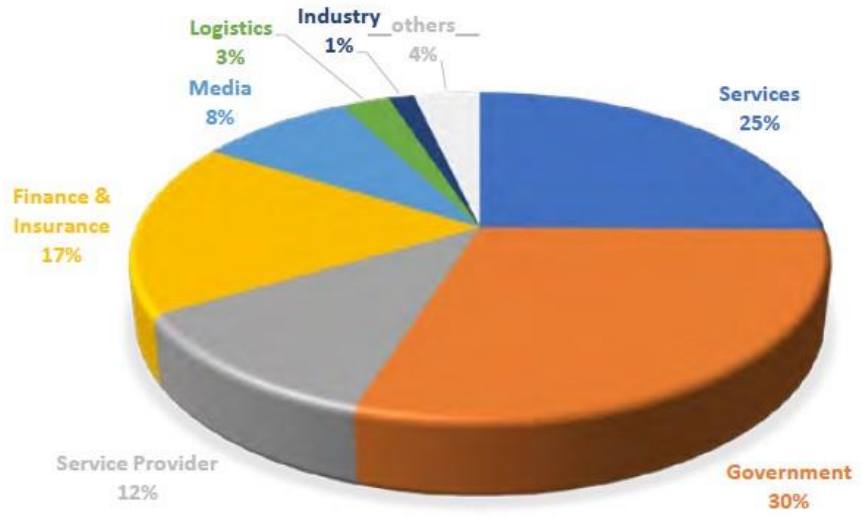
[75] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics guidelines for trustworthy AI*, 08/04/2019.

necessari; peraltro, così formulati, si prestano a interpretazioni troppo vaghe, considerato anche che i produttori implementeranno questi requisiti nella forma tecnicamente più conveniente ed economicamente meno costosa"[76], sicché "è certamente auspicabile che nei prossimi mesi questi requisiti siano rivisti in un'ottica più esplicitamente orientata alla Cyber-security, senza la quale nessuna Artificial Intelligence potrà mai essere davvero affidabile"[77].

Con queste premesse, "la realistica previsione è che dal punto di vista delle minacce alla Cyber-security globale e degli impatti conseguenti, il Machine Learning rappresenti un ulteriore fronte sostanzialmente non presidiato, un Far West tecnologico nel quale la complessità della Supply chain e la mancanza di chiare responsabilità da parte di produttori, gestori e utenti finali, rendono impossibile non solo l'applicazione di contromisure efficaci, ma anche il monitoraggio e la gestione dei rischi associati".

Uno spaccato significativo della situazione in Italia lo danno i numeri e le analisi del Security Operations Center di Fastweb, che nel corso del 2018 ha registrato 40 milioni di Cyber-minacce in rete, in pratica una ogni secondo, in gran parte nei confronti di aziende[78]. Per quanto riguarda gli attacchi DoS (*Denial of Service*), questi puntano a bloccare e mettere fuori uso un computer, una rete o anche solo un particolare servizio, mentre i DDoS (*Distributed Denial of Service*) amplificano la portata di queste minacce. Un attacco DDoS viene infatti realizzato utilizzando delle *Botnet*, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target, con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile. Nel 2018 sono state rilevate oltre 9.300 anomalie riconducibili ad attacchi di questo tipo diretti verso clienti Fastweb (+32% in un anno). I settori più colpiti sono la Pubblica amministrazione (nel 30% dei casi), seguita da Servizi (25%), Finanziario e assicurativo (17%).

[76] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, pag.15.
[77] Ibidem.
[78] F. CERIGNALE, *Cyber security, aumenta la spesa delle imprese italiane (ma è ancora troppo bassa)*, Innovationpost.it, Politiche e tecnologie per l'industria, 05/02/2019.



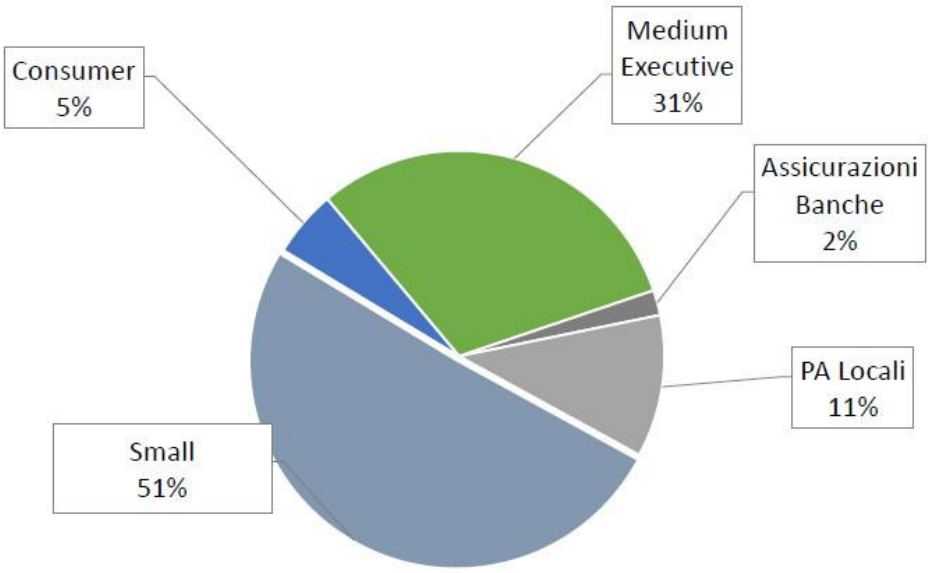
Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2018)

I Service Provider sono il bersaglio prescelto nel 12% dagli attacchi DDoS, mentre si mantengono più bassi quelli nei confronti del settore Media (8%), Logistica (3%), e Industria (solo l'1%)[79].

Anche i servizi VoIp (*Voice over Internet protocol*) possono essere sotto minaccia, e la vulnerabilità del protocollo può rappresentare un ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di Social Engineering e intercettazione, fino a possibili interruzioni di servizio (DoS e DdoS), e *Service Abuse*, dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale.

Sempre secondo i dati raccolti lo scorso anno dal Dipartimento di Fraud Management della Direzione Security di Fastweb, sulle reti della clientela, circa la metà (51%) degli attacchi all'infrastruttura Voip è diretta verso clienti di tipo Small Business (piccole imprese): spesso queste aziende non hanno particolari competenze di tipo tecnico, e il rischio di utilizzare dispositivi non correttamente configurati né monitorati è più elevato rispetto ad altri segmenti di clientela Business. Aziende più grandi, di medie dimensioni, sono il bersaglio nel 31% dei casi, le Pubbliche amministrazioni locali per l'11%, privati cittadini per il 5% del totale.

[79] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, pag. 49.



Vittime di truffe VOIP (Dati Fastweb relativi all'anno 2018)

"Occorre affidarsi a tecnici specializzati, effettuare controlli periodici dei propri dispositivi, ed eseguire anche gli aggiornamenti suggeriti dai produttori. Per ridurre il rischio di intrusione illecita su dispositivi come i centralini digitali, è consigliabile impostare password sicure e aggiornarle periodicamente[80]", sottolineano gli specialisti Fastweb.

5. Il Cybersecurity Act .

Il Cybersecurity Act sta per essere definitivamente attuato ed entrerà nella quotidianità dei cittadini e delle aziende europei[81]. Il nuovo regolamento si compone di due parti: da un lato si vuole creare un quadro europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali; dall'altro viene specificato il ruolo e il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), istituita nel 2004, trasformandola in un'agenzia permanente e autorizzandola ad avere un ruolo operativo[82].

[80] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, pag. 54.
[81] D. BENEDETTI, *Cybersecurity Act, gli effetti della certificazione europea di sicurezza digitale*, Agendadigitale.eu, 12 Apr 2019, pag. 1..
[82] S. DOMINIONI, *Cybersecurity Act: la terza via europea*, Ispionline.it, 12/03/2019, pag. 1..

Il 12 marzo 2019 il Parlamento europeo ha approvato[83] la proposta di regolamento, avanzata dalla Commissione Europea, sulla certificazione di sicurezza informatica delle tecnologie dell'informazione e della comunicazione, abrogando al contempo il regolamento (UE) 526/2013 che rappresentava l'iniziale costituzione dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). L'approvazione del Parlamento fa seguito a un accordo politico tra la Commissione europea, il Parlamento e il Consiglio dell'Unione europea ("Consiglio") raggiunto a dicembre 2018. Per completare il percorso normativo, si attende l'approvazione della proposta di regolamento da parte del Consiglio dell'Unione Europea, in seguito alla quale il regolamento verrà pubblicato nella Gazzetta ufficiale dell'Unione europea.

Volendo schematizzare, il Cybersecurity Act può essere suddiviso in due parti. Nella prima (articoli da 1 a 45) il Regolamento ridefinisce il ruolo e l'organizzazione di ENISA, rendendone permanente il mandato e assegnandole maggiori risorse. ENISA dovrà contribuire ad elevare le capacità di cybersecurity della UE, sostenendo il rafforzamento della preparazione degli Stati membri e delle loro capacità di risposta e costituirà inoltre un centro di competenze indipendente, che si adopererà per promuovere il livello di consapevolezza dei cittadini e delle imprese relativamente alla sicurezza dei dati, aiutando al contempo le istituzioni dell'UE e gli Stati membri nello sviluppo e nell'attuazione delle politiche comunitarie in tale ambito. Infine, ENISA avrà un ruolo chiave nella definizione e nell'implementazione del nuovo schema di certificazioni europee per la cybersecurity.

Nella seconda parte, gli articoli da 46 a 65 istituiscono il quadro europeo di certificazione della cybersecurity, al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di sicurezza e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cybersecurity, così da favorire la creazione e l'armonizzazione di un mercato unico digitale per i prodotti, i servizi e i processi digitali.[84]

---

[83] D. MANISCALCO, *Cybersecurity Act: raggiunto l'accordo delle istituzioni europee. Rafforzata la sicurezza informatica in Europa*, OFCS.Report - Osservatorio-Focus per la Cultura della Sicurezza, 13/03/2019, pag. 1.

[84] Cfr. anche"Una strategia di cybersecurity a livello europeo richiede Importanza della formazione di cittadini e PMI alla "cybersecurity by design" in G. Bruzzone, *Il Mercato unico digitale, cybersecurity e big data*, Assonime e School of European Political Economy LUISS, Roma, 03/10/2018, pag.21.

La costituzione di schemi di certificazione specifici per prodotti e sistemi ICT non è di per sé una novità, infatti, schemi di questo tipo già esistono nella maggior parte degli Stati membri. Ad esempio, in Italia, l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Iscom, operante presso il Ministero dello Sviluppo Economico) già certifica la sicurezza informatica di prodotti e sistemi ICT secondo lo schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione[85].

Il quadro europeo di certificazione della Cybersecurity prevedrà un meccanismo volto a istituire sistemi europei e nazionali di certificazione della cybersecurity finalizzato ad attestare che i prodotti, servizi e processi valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti.

Per quanto riguarda le direttrici di azione tecnologiche ed organizzative, l'articolo 51 è molto articolato[86] nell'individuare le caratteristiche di maggiore interesse:

- al fine della certificazione sarà necessario appurare che i sistemi, servizi o processi siano in grado di proteggere i dati dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita (cfr. anche il "GDPR");
- che siano in grado di proteggere i dati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità;
- che l'accesso di persone, programmi o macchine sia limitato esclusivamente ai dati, ai servizi o alle funzioni per i quali questi dispongono dei diritti di accesso;
- che siano state individuate e documentate le dipendenze e vulnerabilità note e sia possibile registrare a quali dati, servizi o funzioni è stato effettuato l'accesso, in quale momento e da chi;
- deve essere possibile ripristinare tempestivamente la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in caso di incidente fisico o tecnico;

[85] L. TOSONI, *Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT*, Agenda digitale.eu, 13 Mar 2019.

[86] L'articolo 51è intitolato "Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza".

• siano utilizzati criteri di "*security by design*" per la progettazione e che, *by default*, tali prodotti implementino le impostazioni più sicure, ed infine che il software e l'hardware siano costantemente aggiornati per mezzo di meccanismi protetti.

Tenendo conto che non tutti i sistemi, processi e servizi hanno lo stesso profilo di rischio, vengono previsti tre livelli di certificazione differenti (art. 52 commi 5, 6 e 7):

• livello di affidabilità "di base": può bastare un riesame della documentazione tecnica, attività di valutazione sostitutive di effetto equivalente. Il livello base è l'unico per il quale il produttore/fornitore può ricorrere all'autocertificazione, ove prevista.

• livello di affidabilità "sostanziale": la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo i rischi di incidenti ed attacchi informatici commessi da soggetti che dispongono di abilità e risorse limitate. Le attività di valutazione comprendono almeno un test per verificare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti o servizi attuino correttamente le necessarie funzionalità di sicurezza.

• livello di affidabilità "elevato": la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione comprendono: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti attuano correttamente le necessarie funzionalità di sicurezza allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione.

Questo insieme minimo di caratteristiche individua alcuni obiettivi ben precisi per garantire la trasparenza e la verificabilità nell'utilizzo dei dati e delle informazioni generati, utilizzati o trasmessi dai sistemi certificati. In pratica l'obiettivo è quello di rendere evidente e tangibile l'affidabilità, da questo punto di vista, del prodotto o del servizio a cui ci si affida.

Se il "GDPR"[87]è stato un passo fondamentale in direzione dell'*accountability*, è evidente come un "bollino di sicurezza" da un lato garantisca l'utente circa la confidenzialità e trasparenza con cui i dati saranno trattati e dall'altro permetta alle aziende

[87] Parlamento Europeo e Consiglio, *Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali*

di caratterizzarsi in positivo. In più alcuni requisiti minimi come la *security by design* e la *security by default* permettono di rassicurare l'utente finale che la protezione è assicurata anche senza che gli venga richiesto di applicare settaggi ed impostazioni oscuri o poco comprensibili.

Seconda direttrice, individuata dai requisiti minimi definiti nell'articolo 51, è l'affidabilità del prodotto, intesa come la capacità di continuare ad operare, non essere facilmente alterabile e di essere ripristinato celermente. In effetti, la crescente diffusione di sistemi automatici, quali ad es. apparati biomedicali piuttosto che sistemi di guida assistita sulle automobili, rende urgente la creazione e l'adozione di uno schema di certificazioni che possa garantire l'utilizzatore circa il rispetto di alcuni criteri minimi di sicurezza e di affidabilità, così come già fatto, ad esempio, con l'introduzione del marchio "CE" per i fabbricanti di un prodotto regolamentato UE.

La terza ed ultima caratteristica, non disgiunta dalle altre, è costituita dalla garanzia dell'aggiornamento continuo. Si tratta di un'esigenza spesso poco considerata nei prodotti di consumo, di solito venduti come oggetti statici ed "isolati", che non è però accettabile per il mondo dei dispositivi intelligenti: un oggetto in grado di utilizzare protocolli informatici per comunicare con l'esterno, sia esso uno smartwatch, un impianto di allarme o un frigorifero Wi-Fi, anche se al momento del rilascio viene garantito come esente da vulnerabilità non lo rimarrà a lungo, perché nuove vulnerabilità e nuovi sistemi di attacco vengono individuati continuamente. È quindi necessario garantire un processo continuo di verifica e aggiornamento del prodotto stesso, che garantisca che gli opportuni livelli di sicurezza e privacy siano mantenuti nel tempo.

Gli articoli 58-60 del regolamento stabiliscono poi l'organizzazione delle autorità di Certificazione, specificando che ogni stato membro deve dotarsi di una o più Autorità nazionali di certificazione della sicurezza, accreditate presso ENISA e da questa sottoposte ad un regime di controllo sia verticale sia orizzontale fra le altre autorità, per garantire l'uniformità e la regolarità di applicazione dei criteri di certificazione. Le Autorità nazionali hanno sia il compito di rilasciare le certificazioni, sia di vigilare sulla correttezza dell'applicazione delle norme previste dalla certificazione.

Le Autorità nazionali, a loro volta, possono assegnare una delega generale del compito di rilasciare tali certificati europei di cybersecurity a uno o più organismi di

---

dati e che abroga la direttiva 95/46/CE Regolamento Generale sulla Protezione dei Dati) ("GDPR"), 27/04/2016.

valutazione della conformità che potranno accreditarsi presso gli enti nazionali per poter effettuare i controlli previsti per il rilascio ed il mantenimento della certificazione di prodotti o servizi, rilasciando certificati aventi valore nell'intera unione europea.

In realtà non è mancato qualche commentatore[88] che si è spinto a ventilare "il timore è che si creino "certificatori di serie A", particolarmente attenti nell'applicazione di ogni singola richiesta dell'ENISA, e "certificatori di serie B", magari meno attenti alle richieste di certificazione e più propensi, invece, ad attirare l'attenzione delle società produttrici di software e hardware. Un rischio che non possiamo permetterci già oggi e ancor meno nel prossimo futuro".

Da un punto di vista sistematico, va rilevato che con la recente introduzione della direttiva NIS[89] e della GDPR, l'Unione Europea ha mostrato di avere un piano coerente per la protezione delle infrastrutture critiche e della privacy dei propri cittadini. I due strumenti, volti a normare le attività dei grandi attori infrastrutturali (direttiva NIS) o le aziende medio-grandi che raccolgono e trattano dati personali, lasciavano però scoperta l'area dei numerosi dispositivi e servizi di uso comune (ad es. smartwatch o SmartTV), a diffusione crescente ma per i quali spesso oscuri sono i meccanismi di protezione adottati per difendere la privacy dei suoi utilizzatori da eventuali "attori malevoli". Il Cybersecurity Act intende colmare questo divario, fornendo un quadro normativo europeo per certificare il livello di sicurezza offerto dai prodotti, che si configura quindi come un ulteriore strumento volto a favorire una scelta consapevole da parte del cliente/utente ribadendo altresì l'eccellenza europea nella protezione dei diritti digitali dei propri cittadini.

6. Considerazioni finali.

In molti contesti tecnici, come produzione industriale, strutture di contenimento dell'energia nucleare, dispositivi chirurgici, edifici e ponti, "è molto facile vedere i danni eticamente significativi che possono derivare da scarse scelte tecniche così come vedere i benefici eticamente significativi della scelta di seguire le migliori pratiche tecniche conosciute. Tutti questi contesti presentano in pratica evidenti problemi di

[88] I. ORFINO, *Perché l'approvazione del Cybersecurity Act è una buona cosa, ma non è ancora una cosa buona*, Innovationpost.it, Politiche e tecnologie per l'industria, 16/03/2019, pag. 2.

[89] Parlamento Europeo e Consiglio, *Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione* (*'Direttiva NIS''*), 06/07/2016.

‘*vita o morte*”[90]...“*Nel contesto della pratica della cybersecurity, i potenziali danni e benefici non sono meno reali o eticamente significativi, fino a comprendere le questioni della vita e della morte. Ma a causa del fatto che gli sforzi per la sicurezza informatica sono spesso realizzati "dietro le quinte", in gran parte nascosti, la natura etica della pratica della sicurezza informatica può essere più difficile da riconoscere*[91]”.

Purtroppo, però, i danni per le libertà e i diritti delle persone, come si è visto, possono risultare enormi e non solo in termini economici, ma esistenziali e addirittura ontologici. Nella prospettiva classica, come ricordava Baudrillard[92], “la tecnologia è un prolungamento del corpo. Da Marx a MacLuhan le stesse visioni strumentali delle macchine e del linguaggio sono dei ricambi, dei mediatori di una natura idealmente destinata a divenire il corpo organico dell’uomo.” Nella prospettiva cibernetica, invece, “il corpo stesso non è che un medium”. Anzi, in un mondo zeppo di dispositivi IoT, il rischio per l’uomo è che egli stesso diventi un insieme di preziosi sensori per la rete, mentre nell’universo dei *big data* il prezzo per utilizzare app o servizi è spesso molto salato, sebbene non appaia *ictu oculi*, potendosi sostanziare nella fornitura – volontaria a titolo gratuito (o quasi) oppure estorta dai cybercriminali[93]- dei propri dati personali.

Diventa quindi ancor più chiaro che “un ruolo chiave nel sistema è svolto dagli standard relativi alla cybersecurity che sono riconosciuti come una delle priorità della politica europea di standardizzazione in campo ICT, insieme agli standard per 5G, cloud, big data e internet of things, e sono fondamentali per assicurare l’interoperabilità[94]delle soluzioni” che vanno a comporre il quadro complessivo oggetto dell’e-government per come immaginato e auspicato.

[90] S. VALLOR, W.J. REWAK, *An Introduction to Cybersecurity Ethics*, Markkula Center for Applied Ethics at Santa Clara University, California, 07/02/2018, pag.7.

[91] Ibidem.

[92] J. BAUDRILLARD, *Cyberfilosofia*, Mimesis Edizioni, Milano-Udine, 2010, pag. 25.

[93] Accenture Security, *Ninth Annual Cost of Cybercrime Study. Unlocking the value of improved cybersecurity protection*, Accenture.com, Cyber Resilient Business, 06/03/2019, pag.7.

[94] G. BRUZZONE, *Il Mercato unico digitale, cybersecurity e big data*, Assonime e School of European Political Economy LUISS, Roma, 03/10/2018, pag.25.

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*

This work is published under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). You may freely download it but you must give appropriate credit to the authors of the work and its publisher, you may not use the material for commercial purposes, and you may not distribute the work arising from the transformation of the present work.