Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 3-30

Intelligenza artificiale e *Internet of Things*: privacy e responsabilità civile

Chiara Giorgini*

1. *Introduzione*

Prima di affrontare il tema dell'intelligenza artificiale e alcune delle problematiche che ne derivano, è opportuno comprendere cosa essa significhi esattamente.

L'espressione "intelligenza artificiale" (IA) ricomprende programmi e sistemi con funzioni e capacità molto diversi tra loro, «che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»[1]. Si tratta di sistemi software, spesso utilizzati anche in combinazione con hardware, che agiscono nella dimensione fisica o virtuale, percependo l'ambiente circostante, acquisendo dati e interpretando

* *Senior Compliance Officer* in MM S.p.A., si occupa della realizzazione di *compliance audit*, effettua a fianco del Data Protection Officer gli adempimenti previsti dalla normativa in materia di data protection ed eroga corsi di formazione interni all'azienda in materia di privacy e d.lgs. 231/2001. Laureata in Giurisprudenza presso l'Università degli Studi di Perugia nel 2013, ha conseguito l'abilitazione all'esercizio della professione forense e seguito un master in Diritto e Impresa presso il Sole 24 Ore, oltre che corsi di perfezionamento in materia di *data protection* presso l'Università degli Studi di Milano.

[1] Cfr. Commissione Europea, COM (2018) 237 *final*, "Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa", 2018, p. 1. Available at SSRN: https://ec.europa.eu/transparency/regdoc/rep/1/2018/IT/COM-2018-237-F1-IT-MAIN-PART-1.PDF.

informazioni, così da decidere le migliori azioni da attuare per raggiungere l'obiettivo prefissato.

L'apprendimento automatico, il *machine learning*, è una delle applicazioni dei sistemi di IA che ha avuto maggiore sviluppo negli ultimi anni, nella quale gli algoritmi sono addestrati per dedurre determinati modelli partendo da un set di dati: esponendo ripetutamente il sistema a forme esperienziali (ad esempio, osservando enormi quantità di immagini), la macchina viene "allenata" a percepire il proprio ambiente riconoscendo le immagini, intrepretando il linguaggio e monitorando i rischi, così da migliorare la capacità dell'essere umano di interpretare la realtà.

L'applicazione delle tecniche di *machine learning* implica la disponibilità di grandi quantità di basi di dati, che «devono anche essere annotati in modo da consentire alla macchina la piena interpretabilità e utilizzabilità nella fase di apprendimento»[2]: quanto più accurati e adeguatamente annotati sono i dati su cui i sistemi di IA si basano, tanto più gli stessi risulteranno efficaci. Pertanto, il funzionamento dei sistemi di IA, tra cui quelli di *machine learning*, dipende in larga misura dai set di dati utilizzati per addestrarli ed è fondamentale che i dati "di addestramento" siano sufficientemente ampi, ricomprendendo il più vasto numero di scenari possibili[3].

Per garantire lo sviluppo dei sistemi di IA nel lungo periodo, è necessario mettere a disposizione ingenti quantità di informazioni. Al riguardo, occorre ricordare che i dati non sono spesso "liberi", ma detenuti da soggetti, quali le grandi piattaforme online, che li raccolgono grazie all'interazione con gli utenti e al rapporto privilegiato che con gli stessi hanno. Le grandi realtà del settore privato dispongono, infatti, di ingenti quantità di dati, a discapito del settore pubblico.

La Commissione UE ha rilevato la necessità di mettere in atto iniziative a livello europeo per migliorare l'accessibilità ai dati[4], in quanto

[2] Cfr. Gruppo di esperti MiSE sull'intelligenza artificiale, "Proposte per una Strategia italiana per l'intelligenza artificiale", 2020, p. 11. Disponibile al link SSRN: https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf.

[3] Cfr. Commissione Europea, COM (2020) 65 *final,* "Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia", 2020, p. 21. Disponibile al link SSRN: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf.

[4] Cfr. Commissione Europea, COM (2018) 237 *final*, cit., p. 11.

Intelligenza artificiale e Internet Of Things: privacy e responsabilità civile

Il contributo offre una panoramica di alcuni dei principali sistemi di "intelligenza artificiale", analizzando le opportunità legate all'utilizzo degli stessi nella quotidianità, ma anche i relativi rischi. Si vedrà, infatti, come la dipendenza delle tecnologie di intelligenza artificiale dai dati implichi la necessità di tutelare adeguatamente i diritti e le libertà delle persone fisiche cui gli stessi si riferiscono, valutando quali disposizioni del Regolamento (UE) 2016/679 ("GDPR") entrino in gioco e risultino applicabili ai sistemi di intelligenza artificiale. Sarà analizzata anche la nuova proposta di Regolamento Europeo in materia di intelligenza artificiale, che vuole introdurre una serie di norme applicabili ai sistemi di IA, armonizzando le legislazioni degli Stati membri dell'Unione europea.
Ci si soffermerà, poi, sui sistemi IoT più diffusi, quali *smart toys,* sistemi domotici e assistenti digitali, *smart cars*. Ampio spazio sarà, infine, dedicato ai veicoli a guida autonoma, approfondendo le problematiche poste dall'assenza di un adeguato quadro normativo che tuteli il danneggiato in termini risarcitori e valutando che tipo di responsabilità si configuri a fronte di danni cagionati da veicoli parzialmente o totalmente automatizzati.

Artificial intelligence and the Internet of Things: privacy and liability

The contribution offers an overview of some of the main "artificial intelligence" systems, analyzing the opportunities related to their use in everyday life, but also the related risks. In fact, it will be shown how the dependence of these technologies on data implies the need to adequately protect the rights and freedoms of individuals they apply to, assessing which provisions of Regulation (EU) 2016/679 ("GDPR") come into play and are applicable to artificial intelligence systems. It will also be analyzed the new European Regulation on Artificial Intelligence, which intends to introduce a set of rules applicable to AI systems, harmonizing the laws of the EU Member States.
Then, we will focus on the most popular IoT systems, such as smart toys, home automation systems and digital assistants, smart cars. Considerable space will also be dedicated to self-driving vehicles, investigating the problems posed by the lack of an adequate regulatory framework to protect the injured party in terms of compensation and assessing what type of liability is involved in case the of damage caused by partially or fully automated vehicles.

Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 31-46

Intelligenza Artificiale, biometria e indagini di Polizia

Silvestro Marascio*

Sommario: 1. Premessa. – 2. Software di Polizia. – 3. Identificazione biometrica. – 4. Conclusioni.

1. *Premessa*

Il tema dell'IA provoca sicuramente un grande fermento nella società contemporanea, probabilmente è uno degli argomenti sempre più spesso richiamati al grande pubblico, al pari della *blockchain* o degli NFT[1], questo, chiaramente, in funzione dei traguardi tecnologici già raggiunti, ma anche per i benefici potenziali che ancora si potrebbero ottenere.

* Dattiloscopista forense, laureando in Ricerca Sociale Per la Sicurezza Interna ed Esterna, ha ottenuto un Master in Antropologia filosofica e forense, criminologia e tecniche investigative avanzate, perfezionato in scienze criminologiche e criminalistiche, diritto penale dell'informatica, computer forensics e data protection. É responsabile del corso di specializzazione in dattiloscopia della società di formazione "Polis Open learning", docente nei corsi di criminalistica della Ra.Se.T in Roma.

[1] Secondo molti commentatori i trend digitali del 2022 (o comunque già avviatisi e che proseguiranno nel prossimo triennio) sono: *e-commerce*; virtualizzazione; intelligenza artificiale; metaverso; cloud; 5G; smart contract e *insurtech*. Ovviamente, strettamente correlati ai citati temi, seguirà il palesarsi di nuovi rischi per la cyber security, per la *data protection* e non solo. Gli NFT, per esempio, sono diventati argomenti di particolare interesse, anche in funzione della rivisitazione dell'universo social in chiave metaverso, e per la creazione di una sorta di mercato parallelo. Basti pensare al mondo dell'arte, che ha già avuto modo di apprezzare il "Tondo Doni" in formato digitale (la galleria degli Uffizi ha fatto riprodurre la celebre opera michelangiolesca in nove esemplari, una di queste è stata venduta a 240.000 euro, nel 2021) a questo farà seguito l'Arco della Pace di Milano, il primo monumento al mondo a entrare nel metaverso sottoforma NFT, grazie ad un collettivo internazionale di artisti – "Ouchhh" – con sede ad Istanbul, in collaborazione con la Soprintendenza e Comune meneghini. Questo "universo alternativo" ha permesso la nascita della prima piattaforma italiana dedicata agli NFT del mondo dell'arte (ItaliaNFT) e di converso fonti del Ministero della Cultura rendono noto di voler regolamentare questo settore a livello centrale al fine di ridurre l'eccessiva autonomia gestionale dei singoli plessi museali.

doi 10.53148/CD202201002

L'argomento, quindi, ben si presta a spaziare in vari settori, dal mondo dell'industria ai trasporti, dalla progettazione alla sicurezza[2], finanche al settore sanitario[3] o alla giustizia[4]. Aspetto essenziale rimane la centralità del dato, significandone, nel contempo, uno sforzo sotteso all'intersecare segmenti realmente eterogeni: di tipo normativo, macroarea nella quale si pone l'attenzione su verticali come la tutela della privacy[5] e le modalità di raccolta di quelle stesse informazioni[6]; di tipo tecnico, affrontando le potenzialità offerte dall'intelligenza artificiale, ma anche del *machi-*

[2] Si pensi alla verbalizzazione degli automobilisti che insozzano strade e marciapiedi: questo avviene in Gran Bretagna, reso possibile da *LitterCam*, *softerhouse* che ha come obiettivo *l'environmental crime deterrent and asset management solutions powered by AI*.

[3] In Cina, Russia, India, Polonia, Giappone e Corea del Sud sono stati utilizzati connubi di *face recognition* e "telecamere intelligenti" per tracciare le persone contagiate dal Covid-19. L'accelerazione tecnologica ha offerto maggiori strumenti all'assistenza sanitaria: assicurazioni digitali, diagnosi e IA, app per gestire cure, riconoscimento vocale – *smart speaker* – anche integrati con sistemi "a didascalia", per pazienti afoni, come chi è affetto da SLA.

[4] Un prossimo futuro potrà interessare anche la mutevolezza di eventuali reati: nel "tradizionale" mondo dei social network è possibile arrivare a molestie insistenti tra utenti, nel metaverso, quindi in un contesto di realtà immersiva, tali condotte potrebbero anche avere delle prosecuzioni di natura violenta. Ancora, il connubio offerto dal legal tech spazia su paradossi di natura etica (si richiama l'attenzione sulla decisione robotica) e casi estremi di progettualità tecnica, come le difficoltà riscontrabili in sede di processo civile telematico, circa la produzione di particolari formati (tipicamente file audio e video), oppure alla necessità, in sede penale, di ottenere copia degli atti ancora su CD-Rom. Infine, si pensi all'utilizzo di forme di IA ai fini di contrasto all'evasione fiscale, con conseguente confluenza delle evidenze nel processo tributario, seppur nelle more dei criteri desunti dalle sentenze 2936/2019 e 8474/2019 del Consiglio di Stato: principio di imputabilità e pubblicità dello strumento tecnico (si veda anche la Risoluzione del Parlamento Europeo del 16.02.2017, recante raccomandazioni alla Commissione, concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

[5] Il Garante EU della protezione dei dati Wojcieh Wiewiòrowski, in una intervista a «El Paìs», del 23.12.2021, ha osservato come non si avrà mai una situazione in cui la privacy e i dati saranno adeguatamente protetti, proprio a causa di questa complessità, derivante, anche, dalla estrema mutevolezza della tecnologia. Inoltre, continuando, il giurista polacco parrebbe ritenere che l'UE abbia sbagliato nel consentire lo sviluppo di codici di condotta "propri", alle aziende tecnologiche, per la gestione delle informazioni degli utenti.

[6] Per il quale sarebbe opportuno partire dall'assunto che, per meglio comprendere la materia, è necessario rispondere a quesiti del tipo: cosa può definirsi un dato personale? Per quale motivo è necessaria la sua raccolta? Quali tecnologie vengono utilizzate per la raccolta di quelle informazioni? Dove vengono immagazzinati i dati dopo il loro censi-

Intelligenza Artificiale, biometria e indagini di Polizia

L'importanza dell'evoluzione tecnologica è cosa sicuramente nota in tutti i settori, interessando anche campi differenti come la sicurezza dei dati, la protezione della privacy, l'innovazione normativa. Questo articolo cercherà di delineare l'importanza assunta dall'applicazione dell'intelligenza artificiale e della biometria anche nel settore investigativo, con un occhio di riguardo al contesto nazionale, spaziando dall'identificazione dattiloscopia alla *facial recognition*.

Artificial Intelligence, Biometrics and Police Investigations

The technology interests all working fields and its evolution covers various disciplines, like for example security, data protection and regulatory innovation. This paper will describe concrete applications of AI and biometric data (fingerprints analysis, facial recognition and biological information) to police investigation, with a focus on national panorama.

Smart Contracts, Cloud Computing e Data Protection

Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 49-78

Smart contract: software o contratto? Tentativo di applicazione delle norme sulla teoria generale del contratto

Enrico Pernice*

Sommario: 1. Introduzione: origine e nozione degli smart contracts. – 2. La formazione dello smart contract: applicabilità delle norme sulla teoria generale del contratto. – 2.1. La fase delle trattative: le parti contraenti e la tutela del contraente debole. – 2.2 La conclusione dell'accordo. – 2.3. La cessazione del vincolo contrattuale: incapacità a contrarre, vizi del consenso e diritto di recesso. – 3. Conclusioni: la doppia natura degli smart contracts.

1. *Introduzione: origine e nozione degli smart contracts*

Il termine "smart contract" è stato utilizzato per la prima volta nel 1994 dal ricercatore statunitense di informatica e diritto Nick Szabo[1], il quale, nel tentativo di fornirne una primordiale definizione, ha descritto lo smart contract come un protocollo di transazione computerizzato capace di eseguire le condizioni di un contratto[2]. In un successivo paper,

* Laureato con lode presso l'Università degli Studi di Torino, da sempre appassionato alla protezione dei dati personali e alle tematiche giuridiche più innovative, svolge attualmente la pratica forense all'interno del dipartimento IP/TMT & Data Protection dello studio legale Orsingher Ortu - Avvocati Associati.

[1] Cfr. N. Szabo, *Smart Contracts*, 1994, interamente disponibile all'indirizzo: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html; dello stesso Autore si vedano anche "Formalizing and Securing Relationships on Public Networks", 1997, in «First Monday», vol. 2 (n. 9), e *The Idea of Smart Contracts*, 1997, consultabile all'indirizzo: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html, in cui emerge come egli abbia preso spunto dal sistema di vendita dei distributori automatici per teorizzare il trasferimento di alcuni diritti in esecuzione di un algoritmo.

[2] In N. Szabo, *Smart Contracts*, 1994, si legge: «A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens,

lo stesso Szabo ha precisato che siffatto contratto c.d. "intelligente" (*i.e. smart*) deve essere inteso come un insieme di clausole contrattuali incorporate nell'hardware e nel software (e quindi tradotte in un linguaggio informatico), in modo tale da rendere per il trasgressore più costosa – o addirittura insostenibile – la violazione delle stesse[3]. Tuttavia, tale strumento informatico, la cui funzionalità si basa su un'architettura "if – then", cosicché al verificarsi di una determinata condizione X corrisponde l'esecuzione dell'istruzione Y, non ha trovato in un primo momento un supporto in grado di farne decollare l'utilizzo.

Il palcoscenico ideale per un suo utilizzo è emerso soltanto negli ultimi anni con l'avvento delle tecnologie a registro distribuito (cc.dd. *Distributed Ledger Technologies* o, per brevità, DLT) e, in particolar modo, della tecnologia blockchain[4]. Occorre chiarire, fin da subito, che la fami-

confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs».

[3] Cfr. N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 1996, consultabile all'indirizzo: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, in cui si legge: «The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher».

[4] Una piattaforma blockchain è in genere «un database condiviso, decentralizzato, distribuito, criptato, trasparente e resistente alle manomissioni delle transazioni registrate da una rete di computer». L'etimologia stessa del termine ci fa così intendere che si tratta di una "catena" strutturata in tanti piccoli dati definiti "blocchi". Tali blocchi, ciascuno dei quali contenente più transazioni, sono tra loro collegati in modo che ogni transazione eseguita nella rete debba essere validata sulla base di un processo incentrato sul consenso distribuito su tutti i nodi. Cfr. A. Stazi, *Automazione contrattuale e contratti intelligenti*, Torino, Giappichelli, 2019, p. 100. In merito al concetto di decentralizzazione è interessante il contributo di M. Giuliano, "La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio", in «Diritto dell'Informazione e dell'Informatica», vol. II, fasc. 6, 2018, pp. 989 ss., secondo il quale «La blockchain se da un lato è politicamente e architettonicamente decentralizzata, perché nessuno dei partecipanti ha un controllo singolare sulla stessa, e perché la sua infrastruttura non ha un punto centrale di fallimento, poiché ogni nodo conserva una copia della blockchain, dall'altro lato è anche logicamente centralizzata perché il sistema si comporta come un computer nonostante sia distribuito su tutti i nodi partecipanti nella rete. La caratteristica della decentralizzazione consente alla blockchain di essere piuttosto resistente agli attacchi in quanto se uno o più nodi

Smart contract: software o contratto? Tentativo di applicazione delle norme sulla teoria generale del contratto

A seguito della recente diffusione della tecnologia blockchain e degli annessi smart contract, il presente articolo intende offrire una valida e definitiva risposta al quesito circa l'applicabilità, o meno, a tali figure delle norme sulla teoria generale del contratto previste dall'ordinamento giuridico italiano.

Smart contract: software or contract? Attempt to apply the rules on the general theory of contract

Following the recent diffusion of the blockchain technology and of the related smart contracts, this article intends to offer a useful and definitive answer to the question whether or not the rules on the general theory of contract provided by the Italian legal system should be applied to these figures.

Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 79-96

I contratti di cloud computing alla luce dell'entrata in vigore della Direttiva UE 770/2019: *species* del *genus* dei contratti di fornitura di contenuti e servizi digitali?

Nicola Nappi[*]

1. *Nozione e brevi cenni sulle caratteristiche del cloud computing*

Il cloud computing è stato a più riprese qualificato da diverse Autorità[1], e più recentemente è stato definito come un «sistema di servizi offerti *on demand* – attraverso la rete Internet – da un fornitore (*cloud provider*) a uno o più utenti finali, volto all'archiviazione, all'elaborazione e all'uso di dati su computer remoti»[2]. Ma è l'Istituto Nazionale statunitense per

[*] Giurista, Master Universitario in Diritto delle Nuove Tecnologie ed Informatica Giuridica, Corso di Specializzazione in *Regulatory Compliance*, Corso di Perfezionamento in Criminalità Informatica e Investigazioni digitali, Consulente esperto qualificato nell'ambito del trattamento dei dati.

[1] Si vedano le definizioni fornite in *Introduction - Opinion 05/2012 on Cloud Computing* del Working Party 29 del giorno 1 luglio 2012, secondo cui il *cloud computing* coincide con «a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space», nonché in OCSE, *Addressing the Tax Challenges of the Digital Economy*, 16 settembre 2014, secondo cui «Cloud computing is the provision of standardised, configurable, on-demand, online computer services, which can include computing, storage, software, and data management, using shared physical and virtual resources (which, depending on the cloud, could be a single organisation, a community of organisations, the general public, or some combination thereof)».

[2] M. Farina, in G. Ziccardi, P. Perri, *Dizionario Legal tech*, Milano, Giuffrè Francis Lefebvre, 2020, p. 176 e ss.

doi 10.53148/CD202201004

le Norme e la Tecnologia[3] che ha fornito forse la definizione più universalmente accettata[4] del cloud computing, e cioè «un modello per abilitare un accesso ubiquo, conveniente e basato sulle richieste a risorse computazionali condivise (ad es. reti, *server, storage,* applicazioni e servizi) che possono essere rapidamente fornite e rilasciate con il minimo sforzo gestionale o interazione con il fornitore»[5] e che ha, inoltre, delineato cinque caratteristiche fondamentali del cloud computing[6]:

i) l'utente può usufruire delle risorse, unilateralmente e autonomamente, senza la necessità di chiedere l'assistenza o l'intervento umano del *service provider*;

ii) le funzionalità sono disponibili in rete ed accessibili attraverso meccanismi standard che ne promuovono l'utilizzo con diversi dispositivi (PC, tablet e smartphone);

iii) le risorse informatiche del *service provider* sono messe in comune per servire più utenti attraverso un modello multi-utente con diverse risorse fisiche e virtuali assegnate e riassegnate in modo dinamico in base alla domanda;

iv) le risorse vengono fornite e rilasciate, anche in modo automatico, per scalare rapidamente verso l'esterno e verso l'interno in base alla richiesta, al punto da sembrare illimitate e sempre disponibili;

v) i sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse base ad una capacità di misurazione a livello astratto appropriato al tipo di servizio richiesto.

[3] National Institute for Standard and Technology (NIST), organo che pubblica "raccomandazioni" contenenti definizioni ampiamente accettate.

[4] Sull'universalità delle definizioni e raccomandazioni del NIST vedasi *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni* «Sfruttare il potenziale del Cloud Computing in Europa»*, COM/2012/0529 final*, 27/09/2012.

[5] P. Mell, T. Grance, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145, Settembre 2011. Disponibile al seguente indirizzo Internet: https://nvlpubs.nist.fov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. [Consultato il giorno 2 Novembre 2021].

[6] Per un'analisi più approfondita di queste cinque caratteristiche, ossia *l'on-demand self-service*, la *broad network access*, la *resource pooling*, la *rapid elasticity*, e il *measured service* vedasi P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, cit., 5.

I contratti di cloud computing alla luce dell'entrata in vigore della Direttiva UE 770/2019: species *del* genus *dei contratti di fornitura di contenuti e servizi digitali?*

Dopo aver delineato in breve la nozione tecnica di cloud computing, le caratteristiche principali ed i modelli di servizi e di distribuzione del cloud computing, il contributo esamina il negozio di cloud computing, soffermandosi sulla sua natura giuridica alla luce dell'entrata in vigore della direttiva UE 770/2019, che potrebbe rappresentare un punto di svolta del difficile problema della sua qualificazione giuridica. In particolare, tale atto è un contratto, a distanza e virtuale, con il quale il *cloud provider* fornisce all'utente software, piattaforma o infrastruttura "come un servizio" (*SaaS*, *PaaS*, *IaaS*) e che fino ad oggi, nonostante le analogie, non si è riusciti a ricondurre univocamente in uno schema previsto dal legislatore o già ricorrente nella pratica. Ma l'attuazione della citata direttiva potrebbe ragionevolmente far qualificare i contratti di cloud computing quali *species* del *genus* dei contratti di fornitura di contenuti o servizi digitali.

Cloud computing contracts in the light of the entry into force of EU Directive 770/2019: species of the genus *of contracts for the supply of digital content and digital services?*

After having briefly outlined the notion, the actors, the essential characteristics and the service and deployment models of the cloud computing, the essay takes into consideration the legal act of cloud computing focusing on its legal nature, in the light of the entry into force of Directive EU 770/2019, which could be a turning point in the difficult problem of its legal qualification. In particular, this act is a distance and virtual contract with which the cloud provider provides the cloud consumer with software, platform or infrastructure "as a service" (SaaS, PaaS, IaaS) and which, despite the analogies, cannot be assimilated into a scheme envisaged by the legislator or already current in commercial practice. But the implementation of this directive could reasonably qualify cloud computing contracts as *species* of the *genus* of digital content and digital service contracts.

Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 97-112

Il sistema eCall: criticità e implicazioni giuridiche legate alla data protection

Alessandra Salluce*

Sommario: 1. Sicurezza su strada e tasso di mortalità nell'Unione Europea: quadro generale. – 2. Il sistema eCall. – 3. La normativa applicabile e le implicazioni giuridiche legate al trattamento dei dati personali.

1. *Sicurezza su strada e tasso di mortalità nell'Unione Europea: quadro generale*

A partire dal 2018, l'Unione europea ha deciso di fare un grande passo in avanti nell'impiego delle tecnologie a sostegno della sicurezza stradale. In effetti, il problema era avvertito da tempo, anche se, nell'ultimo decennio, le statistiche hanno registrato un significativo calo delle vittime rispetto ai primi anni 2000[1]. Stando a quanto riportato dall'ISTAT, nel 2017 l'Unione ha contato 25.315 decessi su strada, contro i 25.720 del 2016. Ogni milione di abitanti, nel 2017 si contano 49,7 morti per incidente stradale in Europa e 55,8 nel nostro Paese, che, in quell'anno, scende dal quattordicesimo al diciottesimo posto della graduatoria europea.

* Assegnista di ricerca in informatica giuridica presso il Dipartimento Cesare Beccaria dell'Università degli Studi di Milano e Research Fellow dell'ISLC – Information Society Law Center, è abilitata alla professione forense e svolge anche consulenza in qualità di Data Protection Officer presso una struttura sanitaria privata.

[1] Nel confronto tra il 2017 e il 2010 (anno di *benchmark* della strategia europea per la sicurezza stradale) i decessi si riducono del 19,9% a livello europeo e del 17,9% in Italia. Tra il 2010 e il 2017 la riduzione media annua del numero di vittime della strada è stata del 3,1% negli Stati membri e del 2,8% in Italia; variazioni comunque inferiori a quelle che erano state stimate per raggiungere l'obiettivo europeo di dimezzare il numero di morti in incidenti stradali entro il 2020. Cfr. ISTAT, "Incidenti stradali – Anno 2017", 23 luglio 2018. Disponibile in Internet all'indirizzo https://www.istat.it/it/files/2018/07/Incidenti-stradali_2017.pdf.

doi 10.53148/CD202201005

Sulla base dell'articolo 91 del TFUE, che prevede, tra i compiti delle istituzioni europee competenti, la creazione di uno spazio di mobilità sicuro, l'obiettivo prefissato dai Legislatori comunitari era quello di ridurre, entro il 2020, il numero di decessi per incidenti stradali del 50% rispetto al decennio precedente; obiettivo che, purtroppo, non è stato raggiunto, dal momento che tale diminuzione ha registrato un valore – seppure apprezzabile – del 36%. Solo la Grecia (54%) ha superato l'obiettivo, seguita da Croazia (44%), Spagna (44%), Portogallo (43%), Italia (42%) e Slovenia (42%). In totale, nove Stati membri hanno registrato cali del 40% o più[2]. Ad ogni modo, l'intento finale, così come delineato nel Libro bianco del 2011 dal titolo "Tabella di marcia verso uno spazio unico europeo dei trasporti - Per una politica dei trasporti competitiva e sostenibile"[3], è quello di azzerare quasi completamente le vittime entro il 2050.

Nei suoi orientamenti strategici, la Commissione ha definito anche sette obiettivi, per raggiungere i quali prevede di adottare misure nazionali ed europee, conformemente ai principi di responsabilità condivisa e di sussidiarietà. Tali obiettivi comprendono quanto segue: migliorare l'educazione e la formazione degli utenti della strada e rafforzare l'applicazione della normativa stradale; migliorare la sicurezza dell'infrastruttura stradale e dei veicoli; promuovere l'utilizzo dei sistemi di trasporto intelligenti, ad esempio mediante il sistema di chiamata d'emergenza a bordo; migliorare i servizi di soccorso e l'assistenza ai feriti; proteggere gli utenti della strada più vulnerabili, quali pedoni e ciclisti.

In tale contesto, tra le iniziative promosse dall'Unione europea, si menzionano, tra le altre, quelle del 2008 e del 2010 volte alla diffusione dei sistemi ITS[4] (sistemi di trasporto intelligenti) nel trasporto stradale, garantendo la diffusione coordinata e coerente di servizi interoperabili di tale sorta all'interno dello spazio europeo, oltre alla creazione, nel 2003, della piattaforma "eSafety", ridenominata poi "iMobility" dal 2011, per

[2] Statistiche consultabili sul sito della Commissione europea, all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1767.

[3] Documento disponibile in Internet al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52011DC0144.

[4] Gli ITS comprendono, ad esempio, i dispositivi di adeguamento automatico della velocità, i dispositivi per conservare la corsia di marcia, i dispositivi di segnalazione di collisione e i sistemi automatici di chiamata di emergenza in caso di incidente.

Il sistema eCall: criticità e implicazioni giuridiche legate alla data protection

Sulla base della Decisione n. 585/2014/UE e del Regolamento UE n. 2015/758, l'Unione europea, nell'intento di ridurre sensibilmente il numero di vittime per incidente stradale, ha introdotto il sistema eCall (*Emergency Call*), il quale, in caso di incidente grave, è in grado di inoltrare autonomamente una chiamata di soccorso al numero unico europeo 112. Accanto al sistema europeo, obbligatorio su tutti i veicoli la cui costruzione è stata approvata dopo il 31 marzo 2018, ve n'è uno alternativo privato, denominato sistema TPS eCall, che inoltra la chiamata, in prima battuta, a soggetti privati, quali società di assicurazioni, call center automobilistici, etc. Nel presente articolo sono analizzate, nello specifico, tutte le implicazioni giuridiche in tema di data protection connesse all'utilizzo di tali sistemi.

eCall System: critical issues and legal implications related to data protection

On the basis of Decision No. 585/2014/EU and EU Regulation No. 2015/758, the European Union, with the aim of significantly reducing the number of victims of road accidents, has introduced the eCall (Emergency Call) system, which, in the event of a serious accident, is able to autonomously forward a call for rescue to the single European emergency call number 112. Alongside the European system, which is mandatory for all vehicles whose construction has been approved after 31 March 2018, there is an alternative private system, called the TPS eCall system, which forwards the call, in the first instance, to private entities such as insurance companies, car call centers, etc. In this paper, all the legal implications in terms of data protection related to the use of such systems are specifically analysed.

Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), pp. 113-138

Progettare le informative privacy tra tecniche comunicative e legal design

Chiara Vescovi*

1. *Introduzione*

Nel mondo dell'evoluzione digitale e dei cambiamenti repentini dettati dall'avanzare delle tecnologie, i dati personali diventano strumento di scambio monetizzabile per prodotti e servizi. Come spesso accade, al fianco di un crescente interesse economico nascono tutele per le parti deboli coinvolte nel processo, nel caso di specie: i clienti, i consumatori, gli utenti di siti web, genericamente i soggetti interessati. È il concetto di privacy stesso, d'altra parte, a nascere intorno agli individui e per gli individui: Alan Westin nel 1967, in *Privacy and Freedom*, definiva la privacy come «the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others».

È proprio intorno alla figura dell'interessato e alla sua protezione che si rivolgono le protezioni legali nate in materia: già nel 1980 l'Organizzazione per la Cooperazione e lo Sviluppo Economico (in inglese, the Organisation for Economic Co-operation and Development - OECD) rilasciava le prime *Guidelines on the Protection of Privacy and Transborder Flow of Personal data*[1] contenenti i primi principi alla base dell'utiliz-

* Dottoranda in Informatica Giuridica presso l'Università Milano-Bicocca e Cyber Law Consultant per lo spin-off universitario ReD OPEN Srl.

[1] Cfr. OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*, Parigi, 1980.

zo dei dati. Tuttavia, solo nel 2013 l'OECD, consapevole del ruolo chiave che gli individui avevano nella trasmissione dei dati personali, riconosce l'impellente necessità di consentire loro una totale comprensione dei rischi legati alla condivisione di informazioni personali (nel caso di specie, soprattutto online)[2].

Parte dei meccanismi di protezione degli interessati devono, quindi, riguardare anche i meccanismi con cui la condivisione delle informazioni avviene, poiché questa deve responsabilizzare l'individuo, rendendogli possibili scelte consapevoli in merito all'utilizzo dei propri dati. Di pari passo alla necessità di tutelare gli individui da gestioni illecite e/o invasive, proseguono poi approcci *market-driven* al dato personale; tuttavia ci si rende anche conto, che la valorizzazione della protezione dei dati personali potrebbe essa stessa costituire un elemento di differenziazione nel mercato e agli occhi dei consumatori. Sono gli Stati Uniti, in particolare, ad incoraggiare questa visione[3], tramite una serie di iniziative proposte dal "FIPs"[4] (U.S. Department of Housing, Education, and Welfare Fair Information Practices) attraverso una serie di report sottoposti al Congresso[5] e dalla Federal Trade Commission ("FTC"), che, tramite il Bureau of Consumer Protection si fece portavoce alle aziende del concetto per cui consentire ai consumatori di prendere coscienza delle operazioni effettuate sui propri dati personali (in un linguaggio comprensibile e immediato) poteva costituire una modalità di facilitazione dei meccanismi competitivi[6].

Ci si rese ben presto conto che nell'ambito della protezione dei dati personali lo strumento principe per entrare in contatto con gli interes-

[2] «Given the key role that individuals play in transmitting personal data, education and awareness activities may be required to help them better understand the risks involved in posting information about themselves and others online, and further consideration may need to be given to their role in privacy protection frameworks». Cfr. OECD, *The OECD Privacy Framework*, Parigi, 2013, p.98.

[3] Cfr. L.F. Cranor, "Necessary but not sufficient: standardized mechanisms for privacy notice and choice", in «Journal on Telecommunications & High Technology Law», vol.10, no. 2, 2012, p. 278.

[4] Cfr. P.M. Schwartz, D. Solove, *Memorandum on Notice and Choice: Implications for Digital Marketing to Youth,* Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children, 2009.

[5] Cfr. U.S. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, Report to Congress*, 2000.

[6] Cfr. L.F. Cranor, "Necessary but not sufficient: standardized mechanisms for privacy notice and choice", in «Journal on Telecommunications & High Technology Law», vol.10, no. 2, 2012, p. 278.

Progettare le informative privacy tra tecniche comunicative e legal design

L'Articolo ripropone il significato originale di informativa privacy in quanto strumento comunicativo con l'utente, evidenziando come spesso la sua costruzione non utilizzi tecniche comunicative efficienti. L'autrice ripercorre, quindi, soluzioni alternative nate in seno all'Accademia, proponendo modelli più comprensibili per gli utenti. Alla loro costruzione fanno da navigatore gli elementi del *legal design*, che suggeriscono cambiamenti strutturali nella progettazione delle informative. Accanto all'informativa privacy viene, poi, portato ad esempio del cambio di paradigma comunicativo il consenso informato, altro documento obbligatorio, che, come l'informativa, se debitamente progettato, può consentire agli utenti di riappropriarsi del controllo di operazioni che li riguardano, ma che spesso non li vedono protagonisti del processo decisionale. Ad ultimo, ci si rivolge alle aziende, volendo dimostrare come le Informative possano diventare risorse per organizzare i propri trattamenti e dialogare con i propri clienti.

Designing privacy notices between communication techniques and legal design

The article recovers the original meaning of privacy policy, which was intended as a communication tool towards the users, who by fully understanding the processing can maintain their control over it. The structure of the policies hardly respects efficient communication techniques; hence the author retraces some proposals of more comprehensible models for users, originated within the academic environment. Using the elements of legal design, which constitute the navigator of some structural changes in the design of the Policies. Alongside the Privacy policy, the informed consent is taken as an example of a change in the communication paradigm: like the policy, the consent may become an opportunity for users to regain control over operations that concern them but that often do not consider their rightful place in the decision-making process. Finally, it addresses the companies, wanting to demonstrate how the policies can become resources instead of mere legal burdens.