Intelligenza Artificiale, Agenti Software e Diritto

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 399-414

Intelligenza Artificiale e procedimento amministrativo: paura di cadere o voglia di volare?

Enrico Autero, Andrea Castelli*

Indice: 1. Introduzione – 2. Procedimento amministrativo e digitalizzazione – 3. Le recenti sentenze del Consiglio di Stato in materia – 4. Le principali criticità emergenti dalle sentenze in esame – 5. Conclusioni.

1. *Introduzione*

L'anno 2020 verrà senz'altro ricordato per il dilagare dell'epidemia del virus SARS-COV-2, ma lo stesso anno rappresenta un momento cardine di estrema importanza per lo sviluppo della tecnologia dell'Intelligenza Artificiale (o AI). Tra i vari campi di applicazione di tale tecnologia – che sono così tanti da non poter essere nemmeno elencati in questa sede – ve n'è uno di particolare interesse per il diritto e per i propri operatori. Si stanno infatti creando con sempre maggiore frequenza delle relazioni tra l'AI e il mondo del diritto, con tentativi di volta in volta più interessanti e frequenti di porre in stretta correlazione le due realtà, seppur differenti, con l'intento di creare un "dialogo" produttivo. In tal senso, si sono dimostrate di particolare rilevanza una serie di pronunce che il Consiglio di Stato ha reso nel corso dell'ultimo anno, volte ad analizzare il tema dell'applicazione della tecnologia algoritmica al procedimento amministrativo. L'acquisto di centralità della tematica, invero, risulta dimostrato anche dal discorso inaugurale dell'anno giudiziario amministrativo 2020 del Presidente del Consiglio di Stato Filippo Patroni Griffi, focalizzato proprio sulla necessità di disciplinare l'uso dell'AI nei procedimenti delle Amministrazioni Pubbliche[1].

* Avvocati, iscritti all'Ordine degli avvocati di Torino.

[1] Relazione di inaugurazione dell'anno giudiziario 2020 del Consiglio di Stato, capitolo III, lett. b), reperibile sul sito https://www.giustizia-amministrativa.it.

Alla luce dell'estrema attualità e rilevanza della suddetta tematica, gli autori si soffermeranno su come si delinea, ad oggi, il rapporto tra l'intelligenza artificiale e il procedimento amministrativo disciplinato a livello nazionale.

2. *Procedimento amministrativo e digitalizzazione*

La questione della digitalizzazione della Pubblica Amministrazione non è nuova. Come è noto, con la disciplina introdotta dalla Legge 7 agosto 1990, n. 241 si è imposto a livello nazionale il procedimento come modalità ordinaria di esercizio del potere amministrativo. In considerazione del momento storico in cui tale legge è stata promulgata non era immaginabile la possibilità di automatizzare il procedimento grazie all'impiego di tecnologie digitali. Tuttavia, il successivo sviluppo di strumenti sempre più evoluti in ambito digitale ha reso necessario aggiornare la legge n. 241/1990 per evitare un eccessivo distanziamento tra le tecnologie disponibili e la disciplina del procedimento. Una prima riforma in tal senso è avvenuta nel 2005 con l'introduzione dell'art. 3-*bis* nella legge sul procedimento amministrativo, con cui il Legislatore ha incentivato l'utilizzo della telematica nei rapporti tra Amministrazioni e tra privati[2]. A seguito della cd. Riforma Madia della Pubblica Amministrazione[3] si è tentato, poi, di perseguire il principio del *digital first* prefigurando «il passaggio ad un procedimento amministrativo digitalizzato mediante la ridefinizione e semplificazione delle relative regole accompagnate da adeguate misure concernenti l'organizzazione»[4].

[2] La disposizione, composta di un unico comma, prevede che «per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati».

[3] Con tale dicitura si intende fare riferimento alla Legge n. 124/2015 recante "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche".

[4] Sul punto si veda P. Otranto, "Decisione amministrativa e digitalizzazione della p.a.", in «Federalismi.it – Rivista di Diritto Pubblico Italiano, Comparato, Europeo», 17 gennaio 2018.

Intelligenza artificiale e procedimento amministrativo: paura di cadere o voglia di volare?

Il presente lavoro si pone l'obiettivo di indagare gli aspetti critici dell'applicazione della tecnologia algoritmica nel procedimento amministrativo. L'elaborato, prendendo le mosse da alcune recenti pronunce del Consiglio di Stato, propone un'analisi generale in ordine alla tecnologia dell'intelligenza artificiale ed alla sua applicabilità al diritto, con uno specifico focus in relazione al procedimento amministrativo italiano, e con alcuni spunti critici in merito agli aspetti più problematici dell'attuale rapporto tra quest'ultimo e l'AI, e la prospettazione di alcune possibili soluzioni.

Artificial intelligence and administrative procedure: fear of falling or desire to fly?

This paper aims at investigating the critical aspects of the application of algorithmic technology in administrative proceedings. The paper, starting from some recent pronouncements of the Italian Consiglio di Stato, proposes a general analysis of the technology of artificial intelligence and its applicability to law, with a specific focus in relation to the Italian administrative procedure, and with some critical points regarding the most problematic aspects of the current relationship between the latter and the AI, and the prospect of some possible solutions.

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 415-423

Il ruolo degli agenti *software* all'interno della contrattazione cibernetica

Enrico Pernice*

Indice: 1. Introduzione: la contrattazione con agenti *software*. – 2. La formazione del contratto cibernetico: applicabilità delle norme sulla teoria generale del contratto. – 3. La contrattazione cibernetica come espressione di un'autonomia privata procedimentale. – 4. Conclusioni: volontà autonoma o integrazione del contratto?

1. *Introduzione: la contrattazione con agenti software*

L'utilizzo degli agenti artificiali, e in particolare degli agenti *software*, può significativamente incidere sulla conclusione di un contratto, dando vita a quello che – in dottrina – viene più comunemente definito come "contratto cibernetico", intendendosi, per tale, un contratto stipulato tra un soggetto umano e un agente *software* o – addirittura – tra due (o più) agenti *software* come parti contraenti tra loro contrapposte.

Quando pensiamo a un agente artificiale, non dobbiamo immaginare (o almeno non più) un'entità estremamente statica nelle sue funzioni di elaborazione, che si limita a riportare comandi prestabiliti dallo sviluppatore. Al contrario, dobbiamo prendere coscienza del fatto che, un simile agente, è oggi in grado di ricoprire un ruolo attivo anche all'interno di attività dinamiche e difficilmente inquadrabili in rigidi schemi predefiniti: l'utilizzo degli agenti *software* nella più preliminare fase delle trattative, ne rappresenta una chiara testimonianza.

A tal fine, infatti, negli ultimi anni sono stati progettati appositi "*negotiation software agents*" (*NSA*) con lo scopo di aiutare e consigliare le parti contraenti durante la fase propedeutica alla conclu-

* Praticante avvocato, specializzato in data protection e IT law.

sione del vincolo contrattuale[1]. Per un corretto funzionamento, tali agenti devono necessariamente essere dotati di un "modello di processo" che delinea le varie fasi della negoziazione e associa a ciascuna di esse specifiche funzionalità in capo all'agente, e un "protocollo", inteso come un insieme di regole che regolano le attività di elaborazione e comunicazione del *software*, imponendo eventuali restrizioni attraverso la limitazione degli *input* consentiti[2]. Un valido esempio di "modello" può essere – per convenzione – suddiviso in quattro fasi: *i)* una *fase di pianificazione* in cui le parti specificano i loro obiettivi e le loro preferenze. Nel caso in cui siano individuate le controparti, esse sono inoltre in grado di decidere preliminarmente le strategie negoziali da utilizzare, come – ad esempio – la scelta di una particolare tecnica di comunicazione; *ii)* una *fase di definizione dell'agenda* in cui vengono programmati i tempi della negoziazione ed eventuali scadenze; *iii)* una *fase di scambio delle proposte* in cui le parti sono in grado di conoscere i limiti degli altri e di identificare le questioni chiave e le aree critiche di disaccordo. Durante questa fase, le parti realizzano il potenziale di un compromesso e possono discuterne gli aspetti principali; *iv)* una *fase di conclusione della negoziazione* in cui le parti – sulla base del compromesso prospettato – raggiungono un accordo finale. In tale sede, possono anche discutere ulteriori questioni che, tuttavia, non hanno alcun impatto sui negoziati (ad esempio, le modalità di attuazione dell'accordo).

[1] Accanto a questi ultimi, hanno preso piede anche più articolati sistemi di supporto alla negoziazione (*negotiation support systems*, *NSS*), i quali – se implementati all'interno della rete Internet – prendono il nome di "*e-negotiation systems*" (*ENS*). Sul punto, cfr. G. Kersten, "Negotiation Support Systems and Negotiating Agents", 1998. Downloadable at: https://www.researchgate.net/publication/237664717_Negotiation_Support_Systems_and_Negotiating_Agents e G. Kersten. e G. Lo, "Negotiation Support Systems and Software Agents in E-Business Negotiations, The First International Conference on Electronic Business", 2001. Available at: https://interneg.concordia.ca/views/bodyfiles/paper/2001/05.pdf.

[2] Cfr. P. Braun, J. Brzostowski, G. Kersten, J.B. Kim, R. Kowalczyk, S. Strecker e R. Vahidov, "e-Negotiation Systems and Software Agents: Methods, Models, and Applications", 2006. Available at DOI: https://doi.org/10.1007/1-84628-231-4_15.

Il ruolo degli agenti software *all'interno della contrattazione cibernetica*

Il presente articolo si prefigge l'obiettivo di indagare in merito al ruolo degli agenti artificiali all'interno della formazione del contratto cibernetico. In particolare, si cercherà di capire se una fattispecie contrattuale così formatasi necessiti di una disciplina *ad hoc* o se si possa, al contrario, far riferimento alla teoria generale del contratto, addossando – in quest'ultimo caso – agli agenti *software* un ruolo meramente accessorio e ausiliario ai fini della formazione della volontà.

The role of software agents in cybernetic contracts

The aim of this article is to investigate the role of artificial agents in the formation of cybernetic contracts. In particular, it will be attempted to understand whether an agreement thus formed requires an ad hoc discipline or whether, on the contrary, reference can be made to the general theory of the contract, in which case the software agents will play a merely accessory and auxiliary role in the formation of the will.

Cybersecurity e Protezione dei Dati

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 427-450

Le novità sul Fascicolo Sanitario Elettronico (FSE)

Giulia Escurolle*

Indice: 1. Premessa: la sanità digitale. – 2. Il Fascicolo Sanitario Elettronico: caratteristiche e funzione. – 2.1. Consenso ed informativa al trattamento dei dati contenuti nel Fascicolo Sanitario Elettronico. – 2.2. Gli accessi al Fascicolo Sanitario Elettronico e le misure di sicurezza. – 2.3. I diritti riconosciuti all'assistito. – 3. Il Decreto rilancio e le modifiche al Fascicolo Sanitario Elettronico in punto consenso dell'assistito. – 4. La posizione dell'Autorità garante sulla nuova disciplina del Fascicolo Sanitario Elettronico.

1. *Premessa: la sanità digitale*

Come noto, le tecnologie dell'informazione e della comunicazione (TIC) rivestono, già da tempo, un ruolo determinante per la crescita dell'Unione europea e per il generale aumento della produttività.

Nel marzo 2010 la Commissione europea ha lanciato la strategia Europa 2020[1], con l'intento di preparare l'economia dell'UE alle sfide del prossimo decennio, definendo una prospettiva per raggiungere alti livelli di occupazione, produttività e coesione sociale.

Sette le aree di azione delineate dalla Commissione: realizzazione del mercato unico digitale, miglioramento dell'interoperabilità e degli standard, rafforzamento della fiducia e della sicurezza online, promozione di un accesso veloce a Internet disponibile per tutti, incremento degli investimenti in ricerca e innovazione, integrazione, alfabetizzazione e sviluppo delle competenze digitali, attivazione dei benefici dell'ICT per l'Europa.

* Avvocato penalista del Foro di Torino dal 2013; Dottore di ricerca in diritto penale presso l'Università degli Studi di Torino; Assegnista di ricerca in informatica giuridica presso l'Università degli Studi di Milano; Research Fellow dell'Information Society Law Center – ISLC.

[1] Europa 2020 – Una strategia per una crescita intelligente, sostenibile ed inclusiva – COM (2010)2020.

L'Agenda Digitale Europea è una delle sette iniziative faro della strategia Europa 2020 che fissa obiettivi per la crescita nell'UE da raggiungere entro il 2020. Lanciata nel 2010, l'Agenda Digitale Europea propone di sfruttare al meglio il potenziale delle tecnologie dell'informazione e della comunicazione per favorire l'innovazione, la crescita economica e il progresso offerti da un mercato digitale unico. Tale obbiettivo viene perseguito anche in ambito sanitario, mediante l'attuazione di un Piano d'azione "Sanità elettronica" 2012-2020, che prevede una maggiore efficienza del percorso riabilitativo, diagnostico e terapeutico del paziente e conseguente miglioramento della salute dei cittadini, una maggiore trasparenza nelle procedure, l'accesso online sicuro ai propri dati sanitari e la crescita del mercato delle tecnologie informatiche e telematiche dedicate al mondo sanitario.

Nel quadro dell'Agenda Digitale Europea, l'Italia ha sviluppato l'Agenda Digitale Italiana, una strategia nazionale per raggiungere gli obiettivi indicati dall'Agenda Europea, elaborata in collaborazione con la Conferenza delle Regioni e delle Province Autonome. Nell'ambito dell'Agenda Digitale Italiana sono stati predisposti la Strategia per la Crescita Digitale 2014-2020 per il perseguimento degli obiettivi dell'Agenda Digitale, e il Piano Triennale per l'informatica nella Pubblica Amministrazione, che hanno definito le azioni di intervento dedicate all'ecosistema della sanità digitale e le principali soluzioni finalizzate a migliorare i servizi sanitari, limitare sprechi e inefficienze, migliorare il rapporto costo-qualità dei servizi sanitari, ridurre le differenze tra i territori.

All'interno del Piano Triennale sono stati evidenziati alcuni progetti, quali il Fascicolo Sanitario Elettronico (FSE), come esempio di infrastruttura abilitante; il Centro Unico di Prenotazione (CUP), come esempio di semplificazione dell'interazione tra la Pubblica Amministrazione e il cittadino; la telemedicina, come esempio del rapporto con il territorio; l'*e-Prescription*, ovvero la ricetta medica elettronica; la dematerializzazione dei referti e delle cartelle cliniche e la refertazione on line.

Il primo passo importante nel processo di digitalizzazione del settore sanitario si è registrato con l'introduzione del Fascicolo Sanitario Elettronico (di seguito "FSE" o "Fascicolo"), oggetto del presente

Le novità sul Fascicolo sanitario elettronico (FSE)

Il Fascicolo sanitario elettronico, quale obiettivo della sanità digitale, è lo strumento che contiene l'intera "storia clinica" del paziente, garantendo un servizio sanitario più efficiente ed efficace.
L'obiettivo del presente articolo è quello di delineare la funzione ed il contenuto del Fascicolo, i diritti riconosciuti agli interessati e le novità intervenute sulla sua disciplina, a seguito dell'entrata in vigore del Regolamento (UE) 679/2016 e del decreto-legge 34/2020 (c.d. "Decreto rilancio").

Le novità sul Fascicolo sanitario elettronico (FSE)

The "Fascicolo SanitarioEelettronico", as a goal of "digital health", is the tool that contains the patient's "clinical history", created in order to guarantee a more efficient and effective health service.
The aim of this article is to outline the function and the content of the "Fascicolo", the exercise of data subjects' rights and the recent innovations on its discipline, as a consequence of the entry into force of the General Data Protection Regulation (EU) 679/2016 and the decree-law n. 34/2020 (so called "Decreto rilancio").

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 451-488

"Conosci il tuo nemico": un primo approccio tassonomico ai principali attacchi informatici nel settore del *cybercrime* bancario e finanziario

Simone Bonavita, Alessandro Cortina, Elisabetta Stringhi[*]

1. *Premessa*

Nell'ultimo anno abbiamo assistito ad un'inesorabile accelerazione ed evoluzione delle minacce informatiche[1], che incombono

[*] Simone Bonavita, Avvocato del foro di Milano, Professore a Contratto in Trattamento dei dati sensibili e Researcher all'Information Society Law Centre presso l'Università degli Studi di Milano. E' stato Visiting all'European University Institute (EUI) di Firenze.

Alessandro Cortina, Dottore in Sicurezza dei sistemi e delle reti informatiche e Perfezionato in Criminalità Informatica ed Investigazione Digitale presso l'Università degli Studi di Milano.

Elisabetta Stringhi, Dottoressa in Giurisprudenza presso l'Università degli Studi di Milano e Praticante Avvocato in IT Law. E' stata Visiting presso l'Institute for Information Law (IViR) di Amsterdam. Tutti gli autori hanno partecipato alla redazione del presente contributo. Simone Bonavita ha curato premesse, metodologia e conclusioni. Alessandro Cortina si è occupato degli attacchi basati su malware e SIM e della classificazione tassonomica. Elisabetta Stringhi ha approfondito gli attacchi basati su ingegneria sociale.

[1] All'interno dell'articolo si considererà "minaccia informatica" una «*qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone*»; tale

sulla nostra organizzazione sociale, economica e finanziaria, oltre a modellare significativamente il panorama della sicurezza informatica.

Gli operatori della protezione dei dati e della sicurezza informatica si ritrovano a fronteggiare uno scenario che si caratterizza per discontinuità e complessità, poiché gli attaccanti sono costituiti da gruppi disorganizzati ed "artigiani" del *cybercrime*, bensì sono divenuti gruppi strutturati e coordinati di criminalità organizzata, talvolta di scala internazionale, ovvero Stati nazionali dotati di apparati militari e di intelligence, nonché di reti di fornitori e *contractor*, ovvero gruppi civili o paramilitari sponsorizzati da Stati[2].

Gli obiettivi di tali professionisti del cybercrime sono molteplici: a rischio, sostanzialmente continuo, sono *in primis* le strutture, le reti, i server, i client ed i dispositivi mobili.

Soprattutto in ambito finanziario e bancario[3], sono in crescita determinate tipologie di attacco basate su ingegneria sociale e *malware*, sempre più insidiosi e complessi, che riportano in *auge* una considerazione di oltre un decennio fa secondo la quale «l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia»[4].

Nel concreto, in ambito bancario-finanziario, abbiamo assistito all'aumento di attacchi di tipo BEC *(Business E-mail Compromise)* e *Baking Trojan*, con la finalità precipua di entrare in possesso delle credenziali di accesso ai sistemi di pagamento, oppure dei dati delle carte di pagamento delle vittime, di modifica delle credenziali amministrative di singoli sistemi all'insaputa del target. Risultano inoltre in crescita anche gli attacchi basati su SIM, in particolare, gli attacchi di c.d. *swap SIM*, volti a sfruttare le possibilità offerte dai sistemi di doppia autenticazione. L'aumento esponenziale degli attacchi perpetuati e la nascita di nuove metodologie hanno portato, molto spesso, a riconsiderare sia

definizione è contenuta nell'articolo 2, n. 8, del Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019.

[2] Cfr. CLUSIT, *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia*, 2020, p. 7.

[3] Cfr. P. L. Rotondo, "Elementi sul Cyber-crime nel settore finanziario in Europa", in CLUSIT, *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia*, 2020, pp. 95-114.

[4] Cfr. P. Perri, "Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia.", in «Ciberspazio e diritto», 2008, pp. 261-269.

"Conosci il tuo nemico": un primo approccio tassonomico ai principali attacchi informatici nel settore del cybercrime *bancario e finanziario*

Questo contributo si propone di fornire agli operatori del diritto e della sicurezza informatica nel settore finanziario alcune indicazioni utili sui principali attacchi *Social-Engineering based, Malware-based* e *SIM-based,* in evidenza negli ultimi anni. Rispetto a ciascuna tipologia individuata, svolgeremo una disamina della loro possibile definizione, inquadramento, *modus operandi* nonché dei potenziali rischi connessi per la vittima, delineando una tassonomia di tali attacchi.

"Know your enemy": a taxonomy of the principal cyberattacks in the financial cybercrime sector

The aim of this Article is to provide to the legal and cybersecurity operators with some useful indications on Social Engineering, Malware-based and SIM-based attacks, highlighted in recent years. Therefore, with respect to each type, we will examine their possible definition, classification, way of operating, as well as potential risks to the victim, by outlining an overall taxonomy of such attacks.

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 489-512

I danni da condivisione digitale: alcune categorie esemplari

Alba Calia*

Indice: 1. Introduzione. – 2. I danni da condivisione digitale in ambito scientifico e sanitario. – 3. danni da condivisione digitale e la lesione dei diritti della personalità. – 4. I danni da condivisione digitale e la reputazione aziendale. – 5. Conclusioni.

1. *Introduzione*

Il web 2.0. ha assunto la fisionomia di una grande piattaforma di condivisione, sviluppo e aggregazione di informazioni e servizi che garantiscono un alto livello di interazione tra gli utenti. Un cambiamento che, come opportunamente sottolineato dalla letteratura[1], ha generato nel mondo dell'informazione e della comunicazione, sempre più disintermediato, nuove problematiche di distorsione dell'in-

* Avvocato, Cultrice di materia in Informatica giuridica e principi di filosofia del diritto presso l'Università degli Studi di Cagliari, Master di II livello in Diritto della Concorrenza e dell'Innovazione presso la LUISS School of Law.

Il presente scritto s'inquadra nel progetto di ricerca «Profili giuridici dell'automazione e delle nuove tecnologie – Teoria e pratica dei diritti soggettivi nei nuovi scenari tecnologici», finanziato dalla Fondazione di Sardegna.

[1] Cfr., T. Piazza, M. Croce, "Epistemologia delle fake news", «Sistemi intelligenti», Fascicolo 3, dicembre 2019, pp. 439-467; Cfr., M. Cuono, "In principio era il mercato, poi venne la rete. Disintermediazione, spontaneità, legittimità", «Iride», n. 2, agosto 2015; Cfr., G. Riva, *Fake news. Vivere e sopravvivere in un mondo di post-verità*, Bologna, il Mulino, 2018, p. 90.

formazione online come la mala-informazione (*malinformation*), la disinformazione (*disinformation*)[2] e la polarizzazione dei gruppi[3].

In questo contesto si enuclea il concetto di *danni da condivisione digitale*[4] che denota i danni derivanti dalla diffusione per via digitale di informazioni idonee a ledere differenti beni o interessi protetti dall'ordinamento giuridico.

[2] La *mala-informazione* è un fenomeno distorsivo in cui i contenuti informativi sono fondati su fatti reali – spesso privati – ma destrutturati rispetto al contesto a cui si riferiscono in modo da poter divenire virali e divulgati con il preciso intento di danneggiare una persona, un'organizzazione o un Paese, oppure affermare o screditare una tesi. La *disinformazione* si connota dalla manipolazione di contenuti informativi falsi ma suscettibili di essere recepiti come veri dal lettore, deliberatamente creati per danneggiare un bene giuridico (una persona, un gruppo sociale, un'organizzazione o un Paese) o per affermare/screditare una tesi, consapevolmente diffusi per scopi politici, ideologici o commerciali, quasi sempre attraverso piattaforme online che tendono ad aumentarne la propagazione massiva. Cfr., Rapporto del Consiglio d'Europa, "Information disorder: Toward an interdisciplinary framework for research and policy making", commissionato a First Draft e Shorenstein Center on Media, Politics and Public Policy/Harvard Kennedy School e realizzato da Claire Wardle e Hossein Derakhshan, 2017, pp. 20 e ss.; Cfr., AGCOM, *La filiera dei contenuti fake e le strategie di disinformazione online*, nell'ambito del Tavolo Tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali. Delibera 423/17/CONS, 2017, pp. 5 e ss.

[3] La *polarizzazione dei gruppi* avviene quando, a seguito di una discussione all'interno di gruppi con convinzioni, ideologie e credenze affini, si verifica una estremizzazione delle posizioni già precedentemente acquisite dai soggetti e si crea una crescente distanza con coloro che hanno punti di vista e fonti informative diverse. Questo fenomeno si sviluppa in particolar modo all'interno delle *echo chambers* e specialmente nelle *community* online sempre più vaste e nelle quali gli individui possono trovarsi e raggrupparsi grazie ai meccanismi e agli strumenti delle piattaforme (ad esempio, l'uso degli hashtag per segnalare argomenti o punti di vista di vario tipo). La polarizzazione dei gruppi si basa sulla dinamica psicologica del *bias* di conferma e dunque della tendenza umana a selezionare informazioni aderenti al proprio sistema di credenze, determinando negli individui un rafforzamento e una estremizzazione della propria posizione all'interno di un gruppo, sia in ragione di argomentazioni contrarie del tutto limitate o assenti che per questioni reputazionali. Cfr., C. R. Sunstein, *Voci, gossip e false dicerie: come si diffondono, perché ci crediamo come possiamo difenderci*, Milano, Feltrinelli, 2010, pp. 46 e ss.; cfr., C. R. Sunstein, *#Republic. La democrazia nell'epoca dei social media*, Bologna, il Mulino, 2017, pp. 93 e ss.

[4] Cfr., A. Calia, "Le fake news e i danni da condivisione digitale in Italia", in «Ciberspazio e diritto. Rivista Internazionale di Informatica Giuridica», vol. 20, n. 63, dicembre 2019, pp. 369-385.

I danni da condivisione digitale: alcune categorie esemplari

L'articolo mira ad evidenziare come il concetto di danni da condivisione digitale, ossia i danni derivanti dalla diffusione online di informazioni idonee a provocare lesioni a differenti beni o interessi protetti dall'ordinamento giuridico, pur mantenendo i suoi elementi centrali (la *condivisione* digitale attraverso le modalità di inoltro e di interazione sulle varie piattaforme social, la *persistenza* dell'informazione immessa in rete e la *continuità*, da intendersi come la possibilità di replicare potenzialmente all'infinito le azioni di condivisione dei contenuti), assume delle caratteristiche differenti a seconda del bene giuridico leso.
Il presente lavoro delinea tre categorie esemplari di danni da condivisione digitale: la prima riguarda la divulgazione di notizie idonee a provocare un danno alla salute o turbative dell'ordine pubblico; la seconda concerne le conseguenze della diffusione di informazioni lesive dei diritti della personalità, soprattutto la reputazione e l'immagine personale; la terza attiene alla circolazione di notizie dannose per la reputazione aziendale.

The harms of digital sharing: some exemplary categories

The paper aims to highlight how the concept of the digital sharing harms might be characterized by different elements, based on the legal asset damaged. These harms include the damage caused by the online dissemination of information able to cause injury to different asset or interest protected by the legal system, while maintaining their central elements (digital sharing through the methods of forwarding and interaction on the various social platforms, the persistence of the information entered on the network and the continuity, to be understood as the possibility of potentially endlessly replicating content sharing actions).
This work highlights three major categories of damage due to digital sharing. The first one concerns the dissemination of news able to cause damage to the health or public order; the second one concerns the consequences of the dissemination of information which can be harmful to the personality rights; the third one relates to the circulation of news which might be harmful to the corporate reputation.

Ciberspazio e diritto, vol. 21, n. 66 (3 - 2020), pp. 513-541

Il trattamento dei dati personali delle persone decedute. Note in ambito successorio

Giovanni Di Ciollo*

1. *Introduzione*

Con il precedente contributo[1] si è inteso porre all'attenzione del Lettore i profili personalistici della disciplina introdotta dall'art. 2-*terdecies*. Tale secondo contributo si pone in rapporto di complementarietà con il primo, concludendo ed espandendo le riflessioni già sviluppate intorno alla disciplina introdotta dall'art. *de quo*.

I dati personali non sono un ente giuridico di univoca natura, e le disposizioni regolanti la circolazione di informazioni in quanto *dati personali* si prestano altresì ad influire sul regime giuridico della *res* su cui tali dati insistono; al fine di approfondire tali interferenze, è necessario previamente definire lo statuto giuridico delle informazioni e dei dati personali, anche al fine di saggiarne l'eventuale connotazione patrimoniale.

Le tematiche collimano parzialmente con il dibattito avente ad oggetto i fenomeni successori riguardanti beni digitali[2], il quale, difat-

[1] Cfr. G. Di Ciollo, "Il trattamento dei dati personali delle persone decedute. Note in ambito personalistico", in «Ciberspazio e diritto», 2, 2020, p. 315 ss.

[2] Nel panorama domestico si segnalano, tra i più significativi, i seguenti contributi: M. Cinque, "La successione nel "patrimonio digitale": prime considerazioni", in «Nuova g. civ. comm.», 2, 2012, p. 645 ss.; V. Zeno Zencovich, "La successione dei dati personali e nei beni digitali", nota a sent. TAR Sardegna, sez. II, 18 febbraio 2013, in «Riv. giur. sarda», p. 448 ss. Ead., *L'"eredità digitale" alla prova delle riforme*, in T. Pasquino, A.

ti, è germinato precipuamente in relazione a tematiche afferenti alla protezione della riservatezza di soggetti deceduti. Tali ambiti, seppure differenti, sono indissolubilmente intrecciati, talché non si ritiene possibile prescindere da uno scrutinio dei nodi più problematici aventi origine dall'interferenza fra il fenomeno successorio avente ad oggetto beni digitali e la normativa posta a tutela dei dati personali.

2. *L'informazione come bene giuridico*

I dati personali sono attributi della personalità[3], in quanto informazioni riferibili una persona fisica[4]. Ai fini dell'inquadramento giu-

Rizzo e M. Tescaro (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, Esi, 2020, p. 53 ss.; C. Camardi, "L'eredità digitale. Tra reale e virtuale", in «Dir. inf.», 1, 2018, p. 65 ss.; L. di Lorenzo, "Il legato di *password"*, in «Notariato», 2, 2014, p. 144 e ss; G. Marino, "La «successione digitale»", in «ODCC», 1, 2018, p. 167 ss.; G. Resta, "La 'morte' digital", in «Dir. inf.», 6, 2014, p. 891 ss.; Id., "La successione nei rapporti digitali e la tutela post-mortale dei dati personali", in «Contratto e Impresa», 1, 2019, p. 85 ss; I. Sasso, Privacy post-mortem *e "successione digitale"*, in L.C. Ubertazzi (diretti da) *Annali italiani del diritto d'autore, della cultura e dello spettacolo. XXVIII*, Milano, Giuffrè, 2019, p. 553 ss. A livello internazionale si rimanda a: K. Nemeth, J.M. Carvalho, "Digital Inheritance in the European Union", in «EuCML», 6, 2017, p. 253; E. Harbinja, "Digital Inheritance in the United Kingdom", in «EuCML», 6, 2017, p. 253 ss.; A. Berlee, "Digital Inheritance in the Netherlands", in «EuCML», 6, 2017, p. 256 ss.; B. Maeschaelck, "Digital Inheritance in the Belgium", in «EuCML», 1, 2018, p. 37 ss.; M.O. Mackenrodt, "Digital Inheritance in Germany", in «EuCML», 1, 2018, p. 41 ss.; E. Harbinja, *Legal Aspects of Transmission of Digital Assets on Death*, tesi di dottorato, Università di Strathclyde, 2017; Ead., "*Post-mortem* Privacy 2.0: Theory, law and technology", in «International Review of Law, Computers & Technology», 31 (1),2017, p. 26 ss.

[3] L'espressione "attributi della personalità", seppur copiosamente adoperata, non sembra mai essere stata definita in modo analitico; dottrina sul tema con tale espressione si riferisce alle manifestazioni della personalità *oggetto* dei diritti medesimi: tali vengono di norma esemplificati nel «nome, l'immagine, e altri elementi evocativi della dell'identità», G. Resta, *Autonomia privata e diritti della personalità*, Napoli, Jovene, 2005, p. 4; cfr. Id., *L'oggetto della successione: I diritti della personalità*, in G. Bonilini (diretto da), *Trattato di diritto delle successioni e donazioni*, I, *La successione ereditaria*, Milano, Giuffrè, 2009, p. 731; G. Resta, *Dignità, persone, mercati*, Torino, Giappichelli, 2014, p. 96 ss., pp. 123-124; A. De Cupis, *I diritti della personalità*, in *Trattato dir. civ. comm.*, diretto da A. Cicu e F. Messineo, 2ª ed., Milano, Giuffrè, 1982, *passim*; V. Zeno Zencovich, "I negozi sugli attributi della personalità", in «Dir. inf.», 4-5, 1998, p. 545 ss.

[4] Art. 4, comma 1, n. 1), Regolamento (UE) 2016/679.

Il trattamento dei dati personali delle persone decedute. Note in ambito successorio

Le informazioni sono entità di natura multiforme: dal punto di vista strettamente intellettuale, sono informazioni tutti gli enti in grado di essere intesi dalla sfera cognitiva umana; dal punto di vista giuridico, le informazioni rivestono plurime qualificazioni, fra le quali spiccano quella di dato personale e quella di bene digitale. L'idoneità di una medesima informazione ad essere incasellata in entrambe codeste categorie giuridiche reca frizioni fra diversi rami dell'ordinamento, le quali sono precipuo oggetto di disamina del presente contributo.

Data processing of deacesed individuals. Notes on inheritance law

Information is an ambiguous entity: from a strictly intellectual perspective, information is any entity capable of being understood by the human cognitive sphere; from a juridical point of view, information is subjected to several qualifications, among which the most important are information as *personal data* and information as *digital asset*. The suitability of this entity to be framed in both these legal categories causes friction between different branches of the legal system. Such friction and its analysis will be the main topic of this paper.