Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 3-22

Profili di criticità e di invalidità delle norme sanzionatrici del GDPR

Antonio Ciccia Messina*

Sommario: 1. Approccio basato sulla sicurezza. – 2. L'apparato sanzionatorio del Rgpd. – 3.1. Criticità delle disposizioni incolpatrici: condotte impossibili. – 3.2. Criticità delle disposizioni incolpatrici: condotte atipiche. – 3.3. Criticità delle disposizioni incolpatrici: eccessiva dilatazione ambito edittale delle sanzioni. – 4. Riflessi sui procedimenti amministrativi e riflessi processuali. – 5.1. La gestione delle criticità: vaghezza dei precetti. – 5.2. La gestione delle criticità: ambito edittale. – 5.3. La gestione delle criticità: ambito processuale. – 6. Invalidità del Rgpd. – 7. Conclusioni.

1. *Approccio basato sulla sicurezza*

Generalmente si afferma che, confrontato con l'ordinamento previgente, il Regolamento Europeo Generale sulla protezione dei dati personali n. 2016/679 (qui di seguito brevemente "Rgpd") abbia mutato radicalmente il quadro della disciplina dei trattamenti dei dati personali e della disciplina della sicurezza di detti trattamenti.

In via di premessa rispetto all'argomento principale di questo saggio, si precisa che si dissente totalmente da questa impostazione, la quale risulta frutto di una lettura ideologica e non è basata su una rigorosa analisi di stretto diritto positivo.

In proposito si nota, infatti, che nulla di sostanziale sia cambiato rispetto al sistema sicurezza del "Codice della Privacy" (d.lgs. 196/2003), o, se qualcosa è mutato, il risultato è un impoverimento quantitativo e qualitativo.

Il Codice della privacy, soprattutto nella versione anteriore alle modifiche apportate dall'articolo 45 del decreto legge n. 5/2012, infatti, aveva il grosso merito di *aggiungere*, peraltro ai fini meramente penali, le

* Avvocato iscritto all'Ordine di Torino.

doi 10.53148/1059

misure minime all'impianto quadro della sicurezza costruito, esattamente come l'articolo 32 Rgpd, sulle misure idonee ed adeguate, da considerarsi contemporaneamente come piedistallo e traguardo.

Sul punto specifico del raffronto con il Codice della Privacy, nella versione anteriore all'entrata in vigore del d.lgs. 101/2018, va detto a chiare lettere e scritto a caratteri cubitali che:

a) quanto a misure idonee, il Codice della Privacy e il Rgpd hanno la medesima e identica impostazione generale, poiché il Codice della Privacy imponeva "misure di sicurezza idonee" (articolo 31 abrogato d.lgs. 196/2003);

b) le misure minime indicate nell'abrogato allegato "b" al d.lgs. 196/2003 non erano affatto le uniche richieste, ma avevano il pregio di indicare la soglia più bassa, violata la quale scattava la rimproverabilità penale;

c) la idoneità delle misure "idonee" previste dal Codice della Privacy non era cristallizzata in maniera tassativa in nessun catalogo predeterminato e doveva essere valutata utilizzando parametri simili a quelli indicati dall'articolo 32 Rgpd;

d) il Codice della Privacy era più completo e più ricco, poiché indicava *sia* le misure minime (assoggettate all'onere di aggiornamento a cura del legislatore), *sia* le misure idonee;

e) il Codice della Privacy era più rispettoso delle esigenze di garanzia dell'incolpato/imputato, in quanto agganciava il sistema sanzionatorio a precetti chiari e formulati espressamente in via preventiva;

f) il Codice della Privacy non aveva alcuna lacuna di tutela, se confrontato con il Rgpd, poiché la tutela dell'interessato leso da violazioni della sicurezza era correttamente impostata a livello di responsabilità civile, con applicazione della regola dell'inversione dell'onere della prova, in armonia con la disciplina della responsabilità aquiliana derivante dall'esercizio di attività pericolose;

g) il Rgpd, in realtà, ha un atteggiamento pan-sanzionatorio, colloca le sanzioni fino a livelli draconiani, assicura meno garanzie sostanziali e procedurali per l'applicazione delle sanzioni amministrative e, nonostante ciò, non realizza un livello di sicurezza effettiva dell'interessato.

Per quanto nel passaggio da Codice della Privacy a Rgpd, a riguardo dell'impianto sulla "sicurezza", nulla o pochissimo sia cambiato (salvo l'arretramento delle garanzie), nella non condivisibile lettura maggioritaria si prendono le mosse narrando che il Rgpd avrebbe privilegiato un approccio "basato sul rischio".

Profili di criticità e di invalidità delle norme sanzionatrici del GDPR

Il sistema sanzionatorio amministrativo istituito dal Gdpr evidenzia parecchie criticità, sintetizzabili nella imprevedibilità. Dalla vaghezza del Gdpr deriva anche un oscillante orientamento posto in essere dalle autorità di controllo a riguardo della irrogazione delle sanzioni, che si caratterizzano per un livello draconiano.
Sulla base dell'articolo 267 del Trattato sul funzionamento dell'Unione Europea, è la detta imprevedibilità che genera l'illegittimità del Gdpr per violazione dei principi di garanzia a favore del responsabile stabiliti dalla Carta dei diritti fondamentali dell'Unione Europea a dalla Convenzione Europea per la protezione dei diritto umani e delle libertà fondamentali.

Criticality and invalidity profiles of the sanctioning rules of GDPR

The administrative fines system set out by Gdpr highlights several issues, whose main feature is unpredictability. The vagueness of the Gdpr also results in a wavering approach put in place by enforcement authorities in relation to the imposition of fines, which have a draconian maximum.
Accordingly to article 267 of the Treaty on the Functioning of the European Union, is the unpredictability that ends up in causing the illegality of the Gdpr for violation of warranties in favour of the defendants required by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 23-40

La nozione di dato personale. Spunti di riflessione per un approccio interdisciplinare

Francesco Cirillo*

Sommario: 1. Introduzione. – 2. Dati e informazioni. – 3. Ambiguità e paradossi della riferibilità. – 4. Le definizioni di dato e informazione nella fisica contemporanea. – 5. Il contributo della teoria dell'informazione. – 6. Conclusioni.

1. *Introduzione*

La nozione di dato personale appare centrale sia per ragioni di ordine teorico, poiché gran parte della riflessione filosofica, politica e giuridica assume che alcune delle principali questioni contemporanee gravitino intorno alle nuove tecnologie di trattamento dei dati[1], sia però per ragioni di ordine applicativo, perché la stessa regolamentazione dei dati (e segnatamente quella dei dati *personali*) si fonda necessariamente sulla loro definizione. Va però sùbito osservato che nelle coordinate del diritto le definizioni siano qualcosa di diverso rispetto ad altri ambiti disciplinari, perché hanno un carattere necessario e possono dipendere, oltre che dal risultato di un'attività meramente cognitiva, anche da decisioni, e in tal senso possono dirsi *stipulative*.

* Dottorando in *Law and Cognitive Neuroscience* presso l'Università degli Studi Niccolò Cusano - Telematica Roma.

[1] Basti ora il richiamo al quadro tracciato da Y.N. Harari, *Homo deus. Breve storia del futuro* (2015), Milano, Bompiani 2019; sul versante filosofico L. Floridi, *Pensare l'infosfera: La filosofia come design concettuale*, Milano, Raffaello Cortina 2020; su quello giuridico, tra i tanti, i collettanei di F. Pizzetti (a cura di), *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli 2016, e V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli 2019.

doi 10.53148/1060

È chiaro, allora, che questa premessa generale valga anche per le definizioni di dato e di informazione. Un percorso di ricerca sul loro significato, quindi, lungi dal proporsi l'obiettivo di risolvere le questioni ontologiche sottese, può soltanto limitarsi a registrare gli usi diversi, nei diversi contesti storici o disciplinari, per poi avvicinarsi al significato dei termini nel contesto del diritto e proporre – sia pure *in limine* – suggerimenti anche in chiave *stipulativa*[2].

Eppure, l'impossibilità di pervenire a una definizione ultimativa dei concetti di dato e informazione, sia per prudenze metodologiche, sia per ragioni propriamente epistemologiche, non può esimere la ricerca di ambito giuridico dal frequentare la riflessione multidisciplinare sul punto, soprattutto a valle dei diversi apporti confluiti nella cosiddetta filosofia dell'informazione, in modo tale da convalidare o eventualmente riformulare le categorie e i concetti di cui il diritto della protezione dei dati si serve.

Potrebbe dubitarsi dell'opportunità di una simile direzione delle ricerche: eppure, le nozioni di dato e informazione, sia nel diritto sia in altri ambiti – soprattutto in quelli umanistici – sono ormai tanto diffuse quanto ambigue. Né deve stupire che un campo di studi, quale quello della protezione dei dati personali e della *privacy*, non si serva (e forse non si possa servire) di definizioni consolidate e ultimative. Basti un riferimento a un caso noto e analogo nella cultura giuridica: la teoria della proprietà ha dovuto concentrarsi sulla nozione di *res* (materiale o immateriale) non già alle sue origini, ma solo una volta che il progresso scientifico e tecnologico ha introdotto nuovi problemi, che richiedevano quindi uno sforzo definitorio che poteva essere avvertito solo sulla base di una diversa sensibilità. Si pensi all'esigenza di classificare oggetti diversi, quali quelli cui si rivolge la proprietà intellettuale in senso ampio, o quelli più marcatamente fisici (come le *res* materiali, ma anche le fonti energetiche, l'aria o l'acqua). Così, non deve stupire se il diritto non disponga (anche in questo ambito) di definizioni stabili degli elementi fondamentali del suo stesso discorso[3]. Anche in assenza di uno strumentario concettuale ultimativo, infatti, si può regolamentare determinati fenomeni in modo

[2] Sulle definizioni nel diritto, v. *infra*, *sub* n. 8.

[3] Si può pensare al paradosso di Böckenförde sull'incapacità del diritto di dimostrare i propri fondamenti, espresso, *ex multis*, in E.-G. Böckenförde, *Die Entstehung*

La nozione di dato personale. Spunti di riflessione per un approccio interdisciplinare

Le nozioni di dato e informazione spesso costituiscono un presupposto e indiscusso del discorso giuridico. Tuttavia, i saperi scientifici chiamati a renderne una definizione, dall'informatica alla teoria dell'informazione, dalla filosofia dell'informazione alla fisica, dalla statistica alla semiotica, non sembrano affatto convergere su un approccio univoco. Appare centrale, in questo ambito, la questione filosofica della riferibilità di dati e informazioni alla realtà, che ha ampi risvolti di ordine applicativo, anche con riferimento al diritto della protezione dei dati. In questo contributo, ci si propone di definire le linee essenziali di un possibile approccio interdisciplinare al tema.

The notion of personal data. Ideas for an interdisciplinary approach

The notions of data and information often constitute a prerequisite and undisputed element of the legal discourse. However, the scientific knowledge called to define it, from computer science to information theory, from the philosophy of information to physics, from statistics to semiotics, do not seem to converge on a single approach. In this context, the philosophical question of the traceability of data and information to reality appears central and has broad implications on data protection law. In this contribution, we intend to define the essential lines of a possible interdisciplinary approach to the topic.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 41-58

Guardando oltre la criminalità informatica: l'importanza dell'approccio criminologico del "danno sociale" per osservare il ciberspazio con sguardo critico

Anita Lavorgna*

Sommario: 1. Introduzione. – 2. Il concetto di "danno sociale" e la sua rilevanza nel ciberspazio. – 3. La ricerca di nuovi equilibri tra l'amplificazione e la minimizzazione del danno sociale online. – 4. Un esempio di attualità: la disinformazione medica ai tempi della pandemia. – 5. Conclusioni.

1. *Introduzione*

Il ciberspazio, di per sé, è semplicemente uno spazio sociale che collega le persone e facilita il commercio. Tuttavia, alcune delle sue caratteristiche lo rendono particolarmente vulnerabile allo sfruttamento e all'attuazione di innumerevoli comportamenti socialmente dannosi, in modi spesso molto efficaci.

Negli ultimi due decenni ricercatori di diverse discipline (in particolare criminologi e informatici, nella letteratura internazionale) hanno indagato sulla natura parzialmente criminogena del ciberspazio, concentrandosi in un primo momento sui cosiddetti "crimini informatici in senso stretto" (es. hacking, violazioni di copyright) e, più recentemente, su una gamma più ampia di criminalità e devianza informatica (es. pornografia infantile, crimini d'odio, bullismo) – ovvero su quelle attività illecite in cui il contenuto dell'informazione è offensivo o illegale[1].

* Professoressa Associata di Criminologia, Università di Southampton (Regno Unito).

[1] Si veda, a titolo esemplificativo, D.S. Wall, *Cybercrime: the transformation of crime in the information age*, Cambridge, Polity 2007; T.J. Holt (ed.), *Cybercrime through an interdisciplinary lens*, New York, Routledge 2017; E. Martellozzo, Ea. Jane (eds.), *Cybercrime and its victims*, Londra, Routledge 2017; M. Yar, Kf. Steinmetz, *Cybercrime & society*, Londra, Sage 2019.

doi 10.53148/1061

Esistono tuttavia una serie di comportamenti dannosi che si verificano online e che finora, seppur con alcune eccezioni[2], sono sfuggiti all'attenzione criminologica (e, più in generale, delle "scienze sociali" e del diritto). Si tratta spesso di comportamenti che non violano chiaramente una legge (quindi, per definizione, non sono illegali) e potrebbero anche non essere chiaramente etichettati come "devianti" (ad esempio potrebbero essere predominanti in determinate sottoculture).

Parlare di devianza, infatti, sottintende l'esistenza di una "società del consenso"[3] che non rispecchia il dato empirico delle molteplici ed eterogenee comunità online.

Anche questi comportamenti, tuttavia, possono produrre effetti finanziari, psicologici o fisici negativi sia per gli individui che per la società, e per questi motivi la loro accettazione sociale sta cambiando negli ultimi anni[4].

Si consideri, ad esempio, la disinformazione online (i.e., quando vengono condivise informazioni inaffidabili), i cui effetti sociali possono essere fortemente negativi in un contesto in cui il ciberspazio è sempre più utilizzato per sostenere processi decisionali.

Questo contributo, che riprende ed espande considerazioni e contenuti che sono parte di un'agenda di ricerca più ampia[5], verte sul merito di adottare la nozione criminologica (o "zemiologica"[6], per chi preferisce delimitare ulteriormente approcci disciplinari che afferiscono alle stessa grande famiglia delle "scienze sociali") dei "danni sociali" (*social harms*)

[2] Tra le quali non si possono scordare i lavori di G. Stratton, A. Powell e R. Cameron, "Crime and justice in digital society", «International Journal for Crime, Justice and Social Democracy», 6, 2017, pp. 17-33 e di J. Popham, "Microdeviation", «Deviant Behavious», 39, 2018, pp.159-169.

[3] Cfr. T. Parsons, *The structure of social action,* New York-Londra, McGraw-Hill 1937.

[4] Cfr. T. Keipi, M. Nasi, A. Oksanes e P. Rasanen, *Online hate and harmful content. Cross-national perspectives,* Londra, Routledge 2017.

[5] Si veda in particolare A. Lavorgna, *Looking at crime and deviancy in cyberspace through the social harm lens*, in P.S. Leighton, T. Wyatt e P. Davies (eds.) *Handbook of Social Harm*, Londra, Palgrave 2021 e A. Lavorgna, *Information pollution as social harm: Investigating the digital drift of medical misinformation in a time of crisis*, Bingley, Emerald Publishing 2021.

[6] Si veda, per una trattazione recente, V. Canning e S. Tombs, *From Social Harm to Zemiology: A Critical Introduction*, Londra, Routledge 2021.

Guardando oltre la criminalità informatica: l'importanza dell'approccio criminologico del "danno sociale" per osservare il ciberspazio con sguardo critico

Questo contributo discute i meriti dello studiare la criminalità e la devianza online attraverso un approccio criminologico basato sul concetto di "danno sociale", argomentando come attraverso un approccio di studio basato sul concetto di danno sociale anziché un approccio più tradizionale di tipo legalistico sia possibile non solo capire più a fondo le implicazioni sociali di certe scelte politiche di criminalizzazione o *laissez-faire* rivolte a comportamenti online, ma anche affrontare più consapevolmente discussioni in tema di prevenzione, contrasto e mitigazione del danno. Dopo una breve presentazione del concetto di danno sociale, questo articolo discute come alcuni danni che si verificano con mezzi digitali vengano amplificati per promuovere agende guidate da processi di securitizzazione, mentre altri danni tendano ad essere pericolosamente sottostimati. Il contributo si focalizza in particolare sulla disinformazione medica propagatasi online durante la crisi pandemica come esempio di danno sociale difficilmente affrontabile con un approccio di tipo meramente legalistico.

Looking beyond cybercrime: the importance of the criminological approach of "social harm" to observe cyberspace with critical gaze

This contribution discusses the merits of studying (cyber) crime and deviance through the "social harm" approach, arguing that by preferring it to a more traditional legalistic approach it is possible not only to understand more deeply the social implications of certain political choices of criminalization or laissez-faire aimed at online behaviors, but also to better address issues of crime prevention and contrast, and harm mitigation. After a brief presentation of the concept of social harm, this article discusses how some harms occurring by digital means are sometimes amplified to promote agendas led by securitization attempts, while other harms tend to be dangerously underestimated when they occur online. The contribution focuses in particular on the medical disinformation spreading online during the current pandemic crisis as an example of social harm that is difficult to address through a purely legalistic approach.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 59-77

La minaccia del *deepfake* ed i rischi per la cybersecurity delle organizzazioni economiche: un approccio pratico

Elisabetta Stringhi*

Sommario: 1. Un'introduzione al fenomeno del *deepfake*. – 2. La minaccia del *deepfake* nel contesto delle organizzazioni economiche. – 3. Possibili attacchi informatici basati sul *deepfake*. – 3.1. *Spear phishing* e *whaling*. – 3.2. *CEO fraud*. – 3.3. *Vishing*. – 3.4. Aggiramento dei sistemi di riconoscimento facciale. – 3.5. Furto di identità e impersonificazione. – 3.6. Attacco reputazionale. – 4. Possibili misure tecniche e organizzative. – 4.1. Formazione ed approccio umano-centrico. – 4.2. Formazione e policy sull'uso dell'e-mail. – 4.3. Formazione e policy sull'uso dei *social media*. – 4.4. Formazione e policy sull'uso del telefono aziendale. – 4.5. Formazione e policy sull'attacco reputazionale. – 5. Conclusioni.

1. *Un'introduzione al fenomeno del* deepfake

L'evoluzione senza precedenti dell'intelligenza artificiale ha consentito alle tecniche di ingegneria sociale[1] di compiere una svolta significativa.

Una tendenza recente nello scenario degli attacchi informatici riguarda l'utilizzo di file audio, fotografici e/o audiovisivi sintetizzati con il ricorso di particolari tecniche di intelligenza artificiale, come l'*autoencoder*[2] o le

* Praticante avvocato presso Perani Pozzi Associati. Cultrice della materia in Trattamento di dati sensibili presso l'Università degli Studi di Milano.

[1] L'ingegneria sociale fu definita come «l'arte e la scienza di far sì che le persone obbediscano ai tuoi desideri» in G. Harl, *People Hacking: The Psychology of Social Engineering*, Talk at Access All Areas III, 7 maggio 1997. Per una tassonomia tecnica degli attacchi basati su ingegneria sociale, cfr. K. Krombholz, H. Hobel, M. Huber, E. Weippl, "Advanced social engineering attacks", «Journal of Information Security and applications», vol. 22, ottobre 2014, pp. 113-122.

[2] Per un approfondimento tecnico sulla tecnologia *autoencoder*, cfr. T.T. Nguyen, C.M. Nguyen, D.T. Nguyen, S. Nahavandi, "Deep Learning for Deepfakes Creation and Detection: A Survey", «Computer Vision and Pattern Recognition», settembre 2019. Disponibile all'URL: <https://arxiv.org/pdf/1909.11573.pdf>.

Generative Adversarial Networks[3]. Per quanto riguarda i *file* di tipo fotografico, una prima architettura di *Generative Adversarial Networks*, la tecnologia *StarGAN*[4], realizzava immagini di scarsa qualità e, pertanto, facilmente riconoscibili come false. Le successive architetture *StyleGAN*[5] e *StyleGAN 2*[6] hanno consentito di generare contenuti visivi estremamente accurati.

I *file* fotografici sintetizzati, in via automatizzata, possono consistere sia in una sovrapposizione di volti su corpi differenti (*face swap*), sia nella sintesi di immagini originali (*image-generation*). Per quanto riguarda i *file* di tipo audio, con tale tecnologia possono essere sintetizzati nuovi contenuti audio (*speech synthesis*).

Questo fenomeno è comunemente definito con il termine inglese *deepfake*, termine che combina *deep* e *fake*, dal nome dell'omonimo utente di Reddit "Deepfakes", che ne ha reso popolare la creazione e la diffusione[7].

La fattispecie ha destato l'allarme delle Autorità garanti, degli organismi sovranazionali, delle agenzie europee nell'ambito della protezione dei dati e della sicurezza informatica, date le potenzialità di attacco informatico nell'attuale contesto del *cybercrime* finanziario.

Il *deepfake* è stato definito in dottrina come una «tecnica che utilizza l'intelligenza artificiale per combinare e sovrapporre immagini o video originali, ritraenti una persona, con quelli ritraenti qualcun altro, o per

[3] Trattasi di una classe di *deep learning* teorizzata in I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, & Y. Bengio, "Generative Adversarial Nets", «Advances in Neural Information Processing Systems», giugno 2014, pp. 2672-2680.

[4] Cfr. Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, & J. Choo, "Stargan: Unified generative adversarial networks for multi-domain image-to-image translation", «Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition», novembre 2017, pp. 8789-8797.

[5] Cfr. T. Karras, S. Laine, T. Aila, "A style-based generator architecture for generative adversarial networks", «Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition», giugno 2019, pp. 4401-4410.

[6] Cfr. T. Karras, S. Laine, M. Aittala, A. Hellsten, J. Lehtinen, T. Aila, "Analyzing and improving the image quality of StyleGAN", «Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition», dicembre 2019, pp. 8110-8119.

[7] Cfr. H. Ajder, G. Patrini, F. Cavalli, L. Cullen, "The State of Deepfakes: Landscape, Threats, and Impact", 2019. Disponibile all'URL: https://sensity.ai/reports/.

La minaccia del deepfake *ed i rischi per la cybersecurity delle organizzazioni economiche: un approccio pratico*

L'obiettivo di questo articolo è di analizzare possibili attacchi informatici fondati sul *deepfake* ai danni di un'organizzazione economica, per identificare e delineare delle possibili misure tecniche e organizzative adottabili in tale contesto, in un'ottica di prevenzione o di reazione tempestiva e proattiva. Per ciascuna tipologia di attacco informatico basato su *deepfake*, sono suggeriti accorgimenti e procedure concretamente implementabili. In ultima analisi, un approccio umano-centrico risulta essenziale per contrastare i rischi individuati.

Deepfake threat and cybersecurity risks for economic organizations: a practical approach

The aim of this article is to analyze possible cyberattacks based on deepfake against economic organizations, in order to identify and outline possible technical and organizational measures to be adopted in said contexts, for prevention or reaction purposes. The article will provide practical precautions and procedures for each kind of deepfake cyberattack. A human-centric approach ultimately appears to be essential for tackling the addressed risks.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 81-97

OSINT: l'affascinante mondo delle investigazioni sulle fonti aperte per la raccolta di informazioni personali

Manuela Calautti*

Sommario: 1. Un po' di storia. – 2. Che cos'è l'*Open Source Intelligence*. – 3. La classificazione delle fonti. – 4. La forza della prova formata tramite OSINT nel processo penale e civile - cenni. – 5. Alcuni dei tools maggiormente diffusi. – 6. Conclusioni.

1. *Un po' di storia.*

L'intelligence è il servizio – per lo più segreto o riservato – di raccolta di informazioni su persone o enti[1].

Le prime applicazioni di questa attività di raccolta di informazioni si hanno in campo militare, già a partire dagli antichi Egizi, quando, nella guerra tra il regno del faraone Ramsete II e quello ittita, nelle fasi precedenti la battaglia di Qadesh (1296 a.C.), gli storici rilevano tracce di attività di esplorazione che possiamo definire le prime forme conosciute di ricerca informativa[2].

Durante la Seconda guerra mondiale, nel 1941, su ordine del Presidente Roosevelt nasce il FBIS (*Foreing Broadcast Monitoring Service*), con un piccolo ufficio a Portland (Oregon) e 19 strutture regionali, con il compito di registrare, tradurre, trascrivere e analizzare programmi radiofonici stranieri, con lo scopo di capire le intenzioni del nemico, che all'epoca erano i Giapponesi[3].

* Avvocato iscritta all'Ordine di Locri.

[1] Cfr. Vocabolario Treccani, voce Intelligence, https://www.treccani.it/vocabolario/intelligence/

[2] Cfr. Enciclopedia Treccani, https://www.treccani.it/enciclopedia/intelligence_%28Il-Libro-dell%27Anno%29/

[3] Cfr. F. Minniti, S. Ciriello, "Le fonti informative e l'Open Source Intelligence", ricerca CeMiss C8/z per conto del Ministero della Difesa italiano, p. 126.

Terminata la Seconda guerra mondiale, il FBIS proseguì con la sua attività investigativa, mantenendo un ruolo attivo nella gestione della crisi dei missili sovietici a Cuba, con la traduzione simultanea del discorso del Presidente russo *Khrushchev* a Radio Mosca sulla decisione russa di ritirare i missili: tramite questa attività, l'allora Presidente Kennedy ebbe la possibilità di rispondere immediatamente al governo russo, senza dover aspettare il messaggio ufficiale, risolvendo celermente e positivamente una crisi di dimensioni mondiali[4].

Gli ottimi risultati raggiunti negli anni tramite attività di analisi delle fonti aperte, con l'identificazione di 8.000 database commerciali e il monitoraggio di 3.500 pubblicazioni in 55 lingue, portarono, nel 1992, alla creazione di una task force in materia di *Open Source information* e di un *Open Source Coordinator*, nominati dal DCI, il Direttore Centrale dell'*Intelligence Community,* sotto la gestione della CIA[5].

Dopo gli attentati dell'11 settembre 2001, negli U.S.A. si sviluppò un forte dibattito sulle strutture informative e su come queste potessero rispondere alle minacce terroristiche, anche tramite informazioni provenienti da fonti aperte. Fu così che *l'Intelligence Reform And Terrorism Prevention Act* suggerì la creazione, all'interno dell'ufficio del Direttore Nazionale dell'Intelligence, di un centro per coordinare la raccolta, l'analisi, la produzione e la disseminazione delle fonti aperte verso le agenzie facenti parte dell'*Intelligence Community*, recependo così anche le indicazioni contenute nel rapporto finale della Commissione Nazionale sugli attentati dell'11 settembre 2001, che indicava *l'Open Source Intelligence* quale fonte da integrare pienamente nel ciclo informativo e da disseminare verso le strutture informative nazionali e il vertice decisionale[6].

Nasce quindi l'OSC[7], *Open Source Center*, con sede centrale a Lengley nella struttura della CIA e con l'incarico di supportare le esigenze della comunità informativa, del Pentagono, del Dipartimento di Stato e del Dipartimento per la sicurezza interna.

[4] Cfr. la testimonianza dell'Ammiraglio William Studeman, Deputy DCI, al First International Symposium on Open Source Solutions, dicembre 1992, http://www.fas.org/irp/fbis/studem.html

[5] Cfr. F. Minniti, S. Ciriello, op. cit., p. 127.

[6] Cfr. F. Minniti, S. Ciriello, op. cit., p. 130.

[7] Cfr. https://www.opensource.gov

OSINT: l'affascinante mondo delle investigazioni sulle fonti aperte per la raccolta di informazioni personali

Direste mai che l'Open Source Intelligence nasce all'epoca degli antichi Egizi? Ebbene sì! Gli storici rilevano tracce di OSINT già nelle fasi precedenti la battaglia di Qadesh, risalente al 1296 a.C. Dagli antichi Egizi alla CIA, con l'Intelligence Community Directive 301 (ICD), sino ai più recenti tool di ricerca OSINT e ai *Capture The Flag* (CTF) per esercitarsi, sono passati più di due millenni, eppure i concetti di fondo sono gli stessi: ricerca su fonti aperte. Oggi, con l'utilizzo spasmodico di Internet nelle società occidentali, l'attività di OSINT è più semplice rispetto a quella degli antichi Egizi: tutti lasciamo tracce del nostro passaggio sui social, sul cloud, senza neanche farci caso, e siamo facile preda di chi vuole svolgere ricerche OSINT su di noi. I tool in commercio sono tantissimi, e permettono ricerche per nome, indirizzo e-mail, dominio, indirizzo IP, numero di telefono, immagini, metadata, social network. Maltego e FOCA sono i più importanti, soprattutto per un utilizzo professionale. Tool come TinEye, Spiderfoot, DNSlytics, Centralops.net, haveibeenpwned.com, Lookup e OSINT Framework sono comprensibili anche da chi non ha dimestichezza con OSINT, e vuole iniziare ad avvicinarsi alla materia, anche solo per gioco.

OSINT: the fascinating world of investigations on open sources for the collection of personal information

Would you ever say that Open Source Intelligence was born at the time of the ancient Egyptians? Well yes! Historians detect traces of OSINT already in the phases preceding the battle of Quadesh, dating back to 1296 BC. From the ancient Egyptians to the CIA, with the Intelligence Community Directive 301 (ICD), up to the most recent OSINT research tools and Capture The Flag (CTF) to practice, it's been more than two millennia, yet the basic concepts are the same: the gathering of information exclusively from sources that are accessible to the public. Today, with the spasmodic use of the internet in Western society, the activity of OSINT is simpler than that of the ancient Egyptians: we all leave traces of our passage on social networks, on the cloud, without even noticing it, and we are easy prey to who wants to carry out OSINT research on us. The tools on the market are many, and allow searches by name, email address, domain, IP address, telephone number, images, metadata, social networks. Maltego and Foca are the most important, especially for professional use. Tools like TinEye, Spiderfoot, DNSlytics, Centralops.net, haveibeenpwned.com, Lookup and OSINT Framework are understandable even by those who are not familiar with OSINT, and want to start approaching the subject, even just for fun.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 99-120

La prova informatica dell'infedeltà del coniuge nel processo civile: SMS, messaggistica istantanea, e-mail, estratti di pagine web. Un breve *excursus* tecnico e giurisprudenziale

Mariantonella Ninivaggi*

1. *Introduzione*

Nell'ambito del procedimento di separazione con richiesta di addebito al coniuge per infedeltà è ormai frequente l'uso di prove costituite da c.d. "copie" di messaggi elettronici (SMS, messaggi scambiati tramite le applicazioni di messagistica istantanea, e-mail) e/o di c.d. estratti di pagine web volte a dimostrare, appunto, l'esistenza della relazione extraconiugale che sarebbe stata causa della frattura del rapporto.

L'equiparazione di siffatte produzioni – prevalentemente cartacee – a "copie" di messaggistica elettronica, sotto il profilo tecnico e giuridico, e a prove, nel senso sostanziale e processuale, non è però così scontato. Tuttavia, in giurisprudenza si assiste spesso a salti logici e motivazionali che portano alla conservazione e valorizzazione di tali materiali, che, talora per difetto di contestazione, talaltra per effetto di una loro valorizzazione indiretta, altre ancora a causa del loro errato inquadramento, vengono ugualmente posti a base della decisione.

Scopo di questa breve disamina è quello cercare di riscostruire sia in fatto, che in diritto, la natura dei contenuti elettronici veicolati da tali

* Avvocato iscritta all'Ordine di Bologna.

doi 10.53148/1064

strumenti al fine di individuarne le corrette modalità di acquisizione, di conservazione e di introduzione nel processo e di verificarne la possibile tenuta ed efficacia probatoria a sostegno delle relative domande giudiziali.

2. *La natura tecnica e giuridica di SMS, messaggistica istantanea, e-mail, estratti di pagine web*

La messaggistica elettronica e/o la pagina web, così come le loro c.d. copie (in stampa cartacea), vengono comunemente percepite come scritti e, quindi, come prova scritta o documentale; si tratta di una percezione parzialmente corretta che, però, non può soddisfare il giurista. È vero che la definizione di documento generalmente accolta[1] è, in senso ampio, quella di oggetto idoneo a rappresentare un fatto, ma è anche vero che a potere assumere valore probatorio è il documento idoneo a fornire una rappresentazione giuridicamente rilevante[2], quella che cioè consente di ritenere accertata l'esistenza o meno di un fatto nel processo.

A taluni documenti la legge riconosce *ab origine* la funzione di documentare l'esistenza di un determinato fatto – si pensi agli atti pubblici, alle scritture private, etc. – ciò che li differenzia dagli altri strumenti che, essendo nati per fini diversi, assumono la qualifica di documenti giuridicamente rilevanti nell'ambito del processo.

Il documento è quindi preliminarmente un oggetto, caratterizzato da un elemento materiale, ad esempio la carta per il documento cartaceo o il supporto materiale per il documento informatico, e da un elemento immateriale, ossia il suo contenuto.

Il Regolamento eIDAS definisce il documento elettronico come "qualunque contenuto in formato elettronico, quale testo o registrazione sonora, visiva o audiovisiva"[3], mentre il CAD[4] utilizza la definizione per

[1] Cfr. S. Patti, *Libro sesto: tutela dei diritti Art. 2697-2739. Delle prove*, in G. De Nova (a cura di), *Commentario del Codice Civile e Codici Collegati Scialoja-Branca-Galgano*, Bologna, Zanichelli 2015, p. 307 ss.

[2] Cfr. S. Patti, cit., p. 110.

[3] Cfr. Art. 3. n. 35) Regolamento UE n. 910/2014.

[4] Cfr. Art. 1. D.Lgs. 82/2005 (Codice Amministrazione Digitale), come modificato dal D.Lgs. 179/2016.

La prova informatica dell'infedeltà del coniuge nel processo civile: SMS, messaggistica istantanea, e-mail, estratti di pagine web. Un breve excursus *tecnico e giurisprudenziale*

L'articolo esamina le caratteristiche tecniche dei contenuti elettronici, come ad esempio quelli veicolati dalle e-mail, dalla messaggistica istantanea e dagli SMS, nonché di quelli reperibili dalle pagine web, utilizzati come prova nei procedimenti di separazione coniugale, soprattutto ove vi sia la richiesta di addebito al coniuge per infedeltà. L'articolo mira a verificare la possibile riconducibilità di tali contenuti alle categorie tradizionali della scrittura privata e della prova documentale in genere. Nel compiere tale analisi l'articolo fa espresso riferimento alle categorie generali contenute nel Codice civile, come anche alle specifiche previsioni del Regolamento eIDAS e del CAD (Codice dell'Amministrazione Digitale). Vengono inoltre esaminate alcune interpretazioni giurisprudenziali.

The computer proof of the infidelity of the spouse in the civil process: SMS, instant messaging, e-mail, web pages extracts. A brief technical and jurisprudential excursus

This paper is about the technical properties of electronic contents, such as for instance those driven by e-mail, instant messages and short messages, as well as those available in the web, which are used as evidence of proof within marital separation proceedings, especially when there is a charge request for infidelity issued by a party.
More specifically, the paper aims at verifying the potential attribution of said contents to the traditional categories of private contract and documentary evidence. Within such analysis, references are made to the general legal categories provided by the Italian Civil Code, as well as specific rules established by eIDAS Regulation and C.A.D (Digital Administration Code). Some relevant case law are also taken into consideration.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 121-150

L'*Open Source Intelligence* nella ricerca dei minori scomparsi e la prevenzione del fenomeno

Giulia Pesci*

Sommario: 1. Il fenomeno delle persone scomparse. – 1.1 I minori scomparsi. – 2. Gli strumenti di tutela e di contrasto al fenomeno. – 2.1. Il numero unico europeo 116000. – 3. Gli strumenti tecnologici di supporto e ausilio. – 3.1. Il progetto Europol "Stop child abuse - trace an object". – 4. Le tracce lasciate in rete e l'OSINT. – 4.1. L'OSINT per i minori scomparsi e vittime di abusi. – 5. Conclusioni.

1. *Il fenomeno delle persone scomparse*

Il fenomeno delle persone scomparse registra ogni anno cifre considerevoli. Il digitale, e in particolare l'OSINT, sta ricoprendo sempre più un ruolo determinante in merito alle attività di ricerca e per l'elaborazione di nuove e competitive misure di contrasto.

Per inquadrare correttamente il fenomeno è necessario considerare i dati degli ultimi due anni.

Nella ventiquattresima Relazione annuale del Commissario straordinario del governo per le persone scomparse, che raccoglie i dati del periodo intercorso fra il primo gennaio del 2020 e il 31 dicembre dello stesso anno[1], vengono riportati i dati aggiornati al 31 dicembre 2020 e un'intera parte della Relazione fornisce una dettagliata descrizione delle principali iniziative "assunte nel corso dell'anno per far emergere spunti di riflessione che possono costituire motivo di interesse non solo per gli addetti ai lavori, ma anche per coloro che, sempre più numerosi, dimostrano la loro attenzione nei riguardi del fenomeno".

* Dottoressa in Giurisprudenza e *fellow* dell'Information Society Law Center (ISLC) dell'Università degli Studi di Milano. Cultrice delle materie "Informatica Giuridica" e "Informatica Giuridica Avanzata" e vincitrice di una Borsa di studio per laureati promettenti presso l'Università degli Studi di Milano.

[1] Reperibile all'indirizzo https://www.interno.gov.it/sites/default/files/2021-02/xxiv_relazione_annuale_2020_compressed.pdf (consultato in data 30/06/2021).

Il fenomeno non è certo recente, già nel 2011 le Nazioni Unite hanno istituito nella data del 30 agosto la Giornata internazionale per le vittime di sparizione forzata[2] e il 25 maggio è la data nella quale ricorre la Giornata internazionale dei bambini scomparsi. La Polizia di Stato ha definito la ricorrenza del 2021 come "un'occasione per tenere sempre alta l'attenzione su un fenomeno preoccupante"[3].

La Giornata internazionale dei bambini scomparsi è stata istituita in seguito alla decisione dell'allora Presidente degli Stati Uniti Ronald Reagan di riconoscere, a partire dal 1983, il 25 maggio come la Giornata nazionale dei bambini scomparsi, in memoria dell'improvvisa sparizione di Etan Patz, un bambino di soli sei anni che nel 1979 venne visto per l'ultima volta mentre camminava da solo a Manhattan in direzione della fermata dello scuolabus[4]. Qualche anno dopo, nel 2001, la data del 25 maggio venne riconosciuta a livello internazionale come la Giornata internazionale dai bambini scomparsi (International Missing Children's Day).

Dalla Relazione del Commissario straordinario per le persone scomparse emerge che, nonostante le difficoltà riscontrate nel corso del 2020 a causa dell'emergenza sanitaria e del conseguente ricorso in emergenza a tecniche di lavoro da remoto e forme di collegamento telematico, anche dall'analisi dei dati emerge il consolidarsi di un trend presente da tempo e che evidenzia come il divario fra il numero delle persone scomparse e delle persone ritrovate si stia progressivamente restringendo. Nelle pre-

[2] Nel 2006 le Nazioni Unite hanno adottato la Convenzione internazionale per la protezione di tutte le persone dalle sparizioni forzate (International Convention for the Protection of All Persons from Enforced Disappearance), che definisce, all'articolo 2, "sparizione forzata" l'arresto, la detenzione, il rapimento, o qualsiasi altra forma di privazione della libertà da parte di Agenti dello Stato o di persone che agiscono con l'autorizzazione, il sostegno, o l'acquiescenza dello Stato, seguita dal rifiuto di riconoscere la privazione della libertà o dall'occultamento della sorte o del luogo in cui si trova la persona scomparsa, che la pongono al di fuori della protezione della legge. Viene così riconosciuto il crimine di sparizione forzata, sottolineando come tali condotte comportino la violazione di diversi diritti umani fondamentali.

[3] Cfr. "Minori scomparsi: le iniziative per la Giornata internazionale", all'indirizzo https://www.poliziadistato.it/articolo/3860a6243e65fe9796089140.

[4] Per approfondire, si veda R. Rojas, "What Happened to Etan Patz? Unraveling a Nearly 40-Year-Old Case", «The New York Times», all'indirizzo https://www.nytimes.com/2017/01/30/nyregion/what-happened-to-etan-patz.html (consultato in data 30/06/2021).

L'Open Source Intelligence nella ricerca dei minori scomparsi e la prevenzione del fenomeno

"Quando qualcuno scompare", come si intitola l'ultima campagna di comunicazione del Commissario straordinario del governo per le persone scomparse, in Italia e in molti altri Paesi si instaura un sistema di ricerca delle persone coinvolte che richiede l'intervento e il lavoro di rete di diversi operatori e professionisti qualificati. La tecnologia si è rivelata presto essenziale all'interno di tali procedure e contesti, fino ad arrivare ad avere un ruolo determinante nel ritrovamento e nella tutela delle persone scomparse. I minori rappresentano la categoria maggiormente colpita dal fenomeno e in Europa si registrano più di 250.000 casi di scomparsa di bambini ragazzi al di sotto dei diciotto anni di età. Il fenomeno, nonostante gli sforzi messi in campo con sempre più tenacia, sembra lontano da una drastica diminuzione di casi e richiede, pertanto, una continua analisi degli strumenti di ricerca e prevenzione da potenziare o da integrare. Si sta facendo quindi sempre più spazio nel settore l'OSINT, tramite tecniche e procedure che richiedono particolari competenze informatiche ma al tempo stesso alla portata di tutti, portando con sé l'obiettivo, fra gli altri, di aumentare la cooperazione e la collaborazione tra gli operatori coinvolti e la collettività.

Open Source Intelligence in the search for missing children and the prevention of the phenomenon

"When someone goes missing", as the latest communication campaign of the Italian government's Extraordinary Commissioner for missing persons is titled, in Italy and in many other countries a system of searching for those involved is established and it requires the intervention and networking of various operators and qualified professionals. Technology soon proved to be essential within these procedures and contexts, until it came to play an instrumental role in finding and protecting missing persons. Minors represent the category most affected by the phenomenon and in Europe there are more than 250.000 cases of missing children per year. The phenomenon, despite the efforts made with increasing tenacity, seems far from drastic reduction of cases and requires, therefore, a continuous analysis of research and prevention tools to be strengthened or integrated. OSINT is gaining more and more attention in the field, through techniques and procedures that require special computer skills but at the same time affordable for everyone, bringing with it the objective, among others, of increasing cooperation and collaboration between the operators involved and the community.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 153-164

Algoritmi, danno alla persona e nuove soluzioni *legal tech*

Denise Amram*

Sommario: 1. Premessa. – 2. Il *DataJust* francese e le altre iniziative. – 3. La valutazione d'impatto etico-giuridica. – 4. Le prospettive di *legal tech.*

1. *Premessa*

Il tema del danno alla persona alimenta da decenni il dibattito scientifico nazionale e non solo[1].

La necessità, infatti, di tradurre la compromissione dell'integrità psicofisica e delle relative conseguenze sulla persona in un risarcimento monetario, impatta su una pluralità di settori socio-economici con notevoli ricadute in termini di politica del diritto.

Non è questa la sede per ripercorrere l'evoluzione degli istituti che incidono sui profili risarcitori del danno alla salute e di quello non patrimoniale in caso di mancata lesione dell'integrità psicofisica. È sufficiente, tuttavia, elencare alcune problematiche che ricorrono nell'interpretazione degli istituti coinvolti e che hanno indotto gli studiosi a riflettere circa l'opportunità di far uso delle tecniche di intelligenza artificiale come possibile metodo integrativo alle investigazioni in materia[2].

Un primo profilo di criticità emerge in ordine a cosa si intenda per pregiudizio alla persona: l'individuazione delle poste di danno, al di là delle "etichette formali", devono rispondere – per esigenza di certezza del diritto – a categorie omogenee, che non sempre trovano nei testi norma-

* Ricercatrice affiliata presso LIDER-LAB, Istituto Dirpolis e presso il Dipartimento di Eccellenza EMbeDS, Scuola Superiore Sant'Anna di Pisa. Coordinatice dell'Osservatorio sul danno alla persona. Il contributo è elaborato nell'ambito dei seguenti progetti: MSCA-ITN-2020 Legality Attentive Data Scientists GA 956562 e H2020-INFRAIA-2019-1 SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics GA 871042.

[1] Per tutti: F.D. Busnelli, *Il danno biologico. Dal "diritto vivente" al "diritto vigente"*, Torino, Giappichelli 2001 e M. Bargagna, F.D. Busnelli (a cura di), *La valutazione del danno alla salute*, Padova, Cedam 2002.

[2] Si vedano le iniziative nell'ambito del progetto Predictive Justice, sviluppato presso la Scuola Superiore Sant'Anna di Pisa, https://www.predictivejurisprudence.eu/.

tivi o nelle relative interpretazioni, anche nel medesimo ordinamento, definizioni allineate[3].

Un secondo aspetto concerne le modalità, ovvero le condizioni giuridiche, necessarie al fine di accertare la sussistenza di un pregiudizio risarcibile[4]. Tali requisiti variano in osservanza dei paradigmi risarcitori e delle regole di responsabilità civile applicate in un determinato ordinamento[5].

Superati i due profili precedenti, si pone il problema relativo alla quantificazione dei pregiudizi affinché sia garantita l'integralità del risarcimento e l'utilizzo di analoghi criteri di valutazione del danno in modo da dare certezza del diritto[6].

Le questioni accennate sono analizzate attraverso le lenti della *roadmap* per la "Digitalisation of justice in the EU" che favorisce la conversione delle sentenze in dati "leggibili" da sistemi basati su tecniche di machine learning che li rendano, di fatto, accessibili e interoperabili per una pluralità di finalità[7]. La stessa sfida, se letta con le lenti della strategia europea dei dati, si allinea alla formula "as close as necessary, as open

[3] M. Bussani, A.J. Sebok (eds), *Comparative Tort Law - Global Perspectives*, Cheltenham, Elgar 2021; E. Quill, R.J. Friel, Damages and Compensation Culture: Comparative Perspectives, Cheltenham, Elgar 2016.

[4] Per tutti, F.D. Busnelli, *Illecito civile*, in *Enc. giur.*, Vol. XV, Roma, Treccani 1991.

[5] L'evoluzione dell'interpretazione del paradigma risarcitorio da parte del formante giurisprudenziale incide in questa materia in maniera più significativa che nelle altre. Sin da Corte Cost. 26 luglio 1979, n. 87 e 88, in «Resp. civ. prev.», 1979, p. 698 con nota di G. Ponzanelli, *Danno non patrimoniale e danno alla salute: due sentenze della Corte Cost.*, a Corte Cost. 14 luglio 1986, n. 184, in «Foro it.», I, 1986, c. 2976; a Corte Cost. 11 luglio 2003, n. 233, in «Foro it.», 2003, I, c. 2201 con nota di E. Navarretta, *La Corte Costituzionale e il danno alla persona "in fieri"*, quest'ultima confermando i principi di Cass. 31 maggio 2003, nn. 8827 e 8828, in «Danno e resp.», 2003, p. 826 ss. con nota di F.D. Busnelli, *Chiaroscuri d'estate, la Corte di Cassazione e il danno alla persona*; proseguendo con Cass. 11 novembre 2008, nn. 26972-26975, in «Danno e resp.», 2009, p. 19 ss. con note di A. Procida Mirabelli di Lauro, S. Landini, C. Sganga, e Cass. 11 novembre 2019, nn. 28985-28994, in «Guida al dir.», nn. 49-50, 2019, con commento di G. Comandé, in *Danno e resp.*, 2020, pp. 11 ss. con commenti di S. Cacace, D. Amram, A. D'Adda, G. Ponzanelli, A. Procida Mirabelli di Lauro, R. Pucella.

[6] G. Ponzanelli (a cura di), *Il risarcimento integrale senza il danno esistenziale*, Padova, Cedam 2007.

[7] CEPEJ, European judicial systems efficiency and quality of justice, 2018; Rappr. CEPEJ, Charte éthique européenne sur l'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, 4 déc. 2018, pts 146 s.

Algoritmi, danno alla persona e nuove soluzioni legal tech

L'A. illustra le potenzialità e i rischi emergenti dall'applicazione di algoritmi al materiale giurisprudenziale riportando alcuni esempi tratti da esperienze nazionali e non in materia di danno alla persona. Gli spunti di riflessione si orientano verso nuovi possibili usi di soluzioni legal tech in cui la scienza dei dati – purché applicata in maniera affidabile – può supportare un nuovo approccio alle scienze giuridiche.

Algorithms, personal damage and new legal tech solutions

The A. illustrates the potential and risks emerging from the application of algorithms to case-law materials by reporting some examples taken from national and non-national experiences in the field of personal injury damages. The analysis is oriented towards new possible uses of legal tech solutions in which data science – as long as it is trustworthily applied – can support a new approach to legal studies.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 165-203

Una intelligenza artificiale più umana, tra etica e *privacy*

Filippo Lorè*

Sommario: 1. Algoritmi e diritto: cenni introduttivi. – 2. Profili etici e responsabilità. – 3. La regolazione normativa in materia di protezione dati personali nell'intelligenza artificiale. – 4. L'affermazione del *right to explanation*. – 5. Conclusioni.

1. *Algoritmi e diritto: cenni introduttivi*

L'intelligenza artificiale (IA) è stata recentemente definita come «la scienza della produzione di macchine e sistemi volti all'esecuzione di compiti che, qualora realizzati da esseri umani, richiederebbero l'uso dell'intelligenza per risolvere problemi di apprendimento e conoscenza, di ragionamento e pianificazione»[1] o, anche, come il «field that studies the synthesis and analysis of computational agents that act intelligently»[2].

In realtà, il termine IA, con cui si definiscono sistemi intelligenti studiati da un insieme di scienze, teorie e tecniche tra cui logica matematica, statistica, probabilità, neurobiologia computazionale, informatica, è stato coniato negli anni Cinquanta del secolo scorso da John McCarthy, scienziato americano del MIT (*Massachusetts Institute of Technology*) conosciuto come il padre dell'IA[3].

* Docente a contratto per l'insegnamento di Diritto alla protezione dati personali presso il Dipartimento di Informatica dell'Università degli studi di Bari "A. Moro".

[1] Cfr. U. Pagallo, "Intelligenza artificiale e diritto. Linee guida per un oculato intervento normativo", «Sistemi Intelligenti», Vol. 3, dicembre 2017, p. 615, che riprende M.L. Minsky, *Semantic information processing*, Cambridge, The MIT Press 1968.

[2] Cfr. D.L. Poole, A.K. Mackworth, *Artificial Intelligence: Foundations of Computational Agents*, Cambridge, Cambridge University Press 2010, p. 3.

[3] Cfr. J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, "*Una proposta per il progetto di ricerca estiva di Dartmouth sull'intelligenza artificiale*", 31 agosto 1955. Disponibile al link: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html (20 febbraio 2021).

Nonostante gli studi di Alan Turing, finalizzati a raggiungere un sistema intelligente seguendo gli schemi del cervello umano, e di Minsky, il cui lavoro verteva sulle reti neurali, negli anni Sessanta e Settanta l'Ia ebbe un freno, a causa della lentezza dei calcolatori.

Più di recente, ossia nel 2010, l'*Artificial Intelligence*, definita dall'European Commission for the Efficiency of Justice «un insieme di metodi, teorie e tecniche scientifiche il cui scopo è riprodurre, mediante una macchina, le capacità cognitive degli esseri umani»[4], ha avuto un "nuovo impulso", dovuto alla crescente disponibilità di larghezza di banda per il trasferimento dei dati e l'archiviazione dei dati, alle nuove risorse computazionali e alla progressiva "datificazione" di gran parte della nostra vita e dell'ambiente antropizzato[5].

Dalla disponibilità di nuovi ed enormi volumi di dati e dall'altissima efficienza dei processori di schede grafiche, nell'accelerare il calcolo degli algoritmi di *machine learning* ("ML", sistemi ad apprendimento automatico) a costi contenuti, è derivato un repentino e notevole incremento dei finanziamenti nel settore dell'IA.

Nondimeno, con l'incedere della rivoluzione tecnologica, che consente ai processori di governare ormai ogni tipo di macchina, profondi cambiamenti hanno toccato il modello economico e soprattutto quello sociale, sebbene il grado evolutivo dell'intelligenza artificiale, attualmente, sia unanimemente stabilito ad un livello intermedio di ricerca (IA "debole") e non al suo stadio finale (un'IA "forte", ovvero la capacità di contestualizzare problemi specialistici molto diversi in modo totalmente autonomo)[6].

[4] Cfr. European Commission For The Efficiency Of Justice (Cepej), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2019, p. 69. Disponibile al link https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment, (20 febbraio 2021).

[5] Cfr. A. Mantelero, *Intelligenza artificiale e protezione dei dati: sfide e possibili rimedi*, Relazione di Alessandro Mantelero al «*Rapporto sull'intelligenza artificiale*» del Comitato consultivo della Convenzione per la protezione dei singoli per quanto riguarda l'elaborazione automatica dei dati personali, Strasburgo, 25 gennaio 2019, p. 2.

[6] Cfr. Consiglio d'Europa, *Cos'è l'IA - Storia dell'intelligenza artificiale*. Disponibile al link https://www.coe.int/en/web/artificial-intelligence/history-of-ai, (20 febbraio 2021).

Una intelligenza artificiale più umana, tra etica e privacy

Il presente lavoro fotografa l'evoluzione della giovane e dinamica disciplina che ha come oggetto l'*Intelligenza Artificiale* e ne registra il graduale percorso che essa oggi compie verso una maturità teorica-strutturale sempre più definita. In particolare, la trattazione si sofferma sul problema etico che emerge dall'applicazione dell'*Artificial Intelligence* alle diverse sfere dello scibile umano e sulle possibili soluzioni dettate dalla normativa in materia di protezione dati personali.

A more human artificial intelligence, between ethics and privacy

This work photographs the evolution of the young and dynamic discipline that has Artificial Intelligence as its object and records the gradual path that it now takes towards an increasingly defined theoretical-structural maturity. In particular, the discussion focuses on the ethical problem that emerges from the application of Artificial Intelligence to the different spheres of human knowledge and on the possible solutions dictated by the legislation on personal data protection.

Ciberspazio e diritto, vol. 22, n. 67 (1 - 2021), pp. 205-232

Sistemi di intelligenza artificiale e responsabilità dell'avvocato

Irene Negri*

Sommario: 1. Strumenti di *legal tech* e intelligenza artificiale. – 2. La responsabilità civile dell'avvocato e il Codice civile. – 3. La responsabilità disciplinare dell'avvocato e il Codice deontologico forense. Autonomia dell'azione disciplinare. – 4. Il dovere di competenza. – 5. Il dovere di informazione. – 6. Il dovere di riservatezza. – 7. Il dovere di indipendenza. – 8. La responsabilità dell'avvocato per l'utilizzo di sistemi di intelligenza artificiale. – 9. Conclusioni.

1. *Strumenti di* legal tech *e intelligenza artificiale*

Nel presente Articolo si vuole approfondire il tema relativo alla responsabilità dell'avvocato che, nello svolgimento della propria attività professionale in ambito sia giudiziale che stragiudiziale, si trovi ad utilizzare strumenti legal tech.

Ci si vuole quindi riferire alla responsabilità professionale degli avvocati che godano dello specifico titolo, mentre si tralascerà di considerare le attività degli altri professionisti, che pure talvolta offrono una consulenza *latu sensu* legale (in ambito stragiudiziale).

Il legal tech promette innovazioni dirompenti nel settore della consulenza legale. Innovando la professione degli avvocati, l'introduzione di nuove tecnologie avrà man mano un impatto sempre maggiore anche sulla vita di tutti i cittadini, andando ad incidere sulle modalità e sui mezzi a disposizione per tutelare i loro diritti.

Il legal tech può essere definito come l'insieme degli applicativi e delle soluzioni tecnologiche, specialmente sotto forma di software, dedi-

* Avvocato presso il Foro di Padova. Ha svolto diversi corsi relativi al diritto IT e alla protezione dei dati personali, tra cui il corso Coding for lawyers e Legal tech dell'Università di Milano, al quale sono in parte ispirati i contenuti del presente Articolo.

doi 10.53148/1068

cate a digitalizzare, automatizzare, razionalizzare o semplificare attività e processi nell'ambito delle professioni legali[1].

Il legal tech si compone, in realtà, di alcuni strumenti che possono essere utili per diversi settori di attività, come quelli che permettono di utilizzare la firma elettronica, e di altri più specifici e dedicati al settore legale. Tra questi si ritrovano, in particolare, strumenti per gestire il ciclo di vita dei contratti ("contract lifecycle management"), per l'analisi di documenti mediante l'utilizzo di intelligenza artificiale e machine learning, per l'informatica forense, oltre che per la ricerca giuridica.

In tutti questi settori, il mercato è già in grado di offrire anche strumenti che integrano sistemi di intelligenza artificiale.

Uno dei modi possibili per definire l'intelligenza artificiale, proposto dalla Commissione europea, vede in essa un termine indicante "sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)"[2].

Nel settore legal tech, quando si utilizzano sistemi di intelligenza artificiale, questi sono perlopiù riconducibili alla prima categoria, essendo rappresentati principalmente da software e non da robot "fisici", che risultano invece più diffusi in altri settori. L'intelligenza artificiale può essere sfruttata da una grande varietà di strumenti legal tech, come quelli che permettono, a mero titolo esemplificativo, la *document automation*, la *e-discovery*, la gestione dei contratti o la revisione contrattuale, i quali presentano diversi livelli di autonomia e di "spiegabilità" ("explainability").

Un altro esempio di strumenti legal tech che sfruttano l'IA è rappresentato da quelli che permettono la "legal analytics" e quindi la predizio-

[1] Cfr. G. Ziccardi, P. Perri (a cura di), *Dizionario Legal Tech*, Milano, Giuffrè 2020.

[2] Cfr. Commissione Europea, 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, COM(2018) 237 final, Bruxelles, 25 aprile 2018.

Sistemi di intelligenza artificiale e responsabilità dell'avvocato

Gli strumenti di legal tech promettono innovazioni dirompenti nel settore della consulenza legale e molti di questi integrano anche sistemi di intelligenza artificiale, permettendo di automatizzare parte del lavoro degli avvocati.
Il contenuto degli obblighi posti in capo agli avvocati dal Codice civile e dal Codice deontologico deve essere probabilmente in parte ridefinito alla luce dell'utilizzo di tali strumenti tecnologici e così anche la definizione del regime di responsabilità di chi se ne serva. In particolare, il dovere di competenza dell'avvocato potrebbe ricomprendere il dovere di "competenza tecnologica"; il dovere di informazione potrebbe implicare anche il dovere di ottenere il consenso dei clienti per l'impiego di sistemi di IA; il dovere di riservatezza potrebbe richiedere il rispetto di obblighi ancora più stringenti, mentre il dovere di indipendenza potrebbe essere messo a rischio dalla presenza di *bias* nei sistemi utilizzati nello svolgimento della consulenza legale.

Artificial intelligence systems and lawyers' civil liability

Legal tech instruments promise disruptive innovations in the field of legal advice and many of them incorporate already artificial intelligence systems, which may automate some tasks of the lawyers.
The content of the obligations of lawyers arising from the Italian Civil Code and from the Code of Conduct for lawyers should be probably redefined considering the use of technological instruments, together with the possible liability regimes of their users. More specifically, the duty of competence may include the duty of "technological competence"; the duty of information towards the client may imply obtaining the consent of the clients as regards the use of AI systems; the duty of confidentiality may require the respect of more stringent obligations and, lastly, the duty of independence may be put at risk by the biases, which are present in some of the instruments used in the legal advice activities.