Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 9-23

Fiducia nell'algoritmizzazione della Pubblica Amministrazione: chimera o realtà?

Jean Louis a Beccara*, Silvio Ranise**

Indice: 1. Inquadramento. – 2. Processo all'algoritmo. – 3. Una difficile traduzione tecnica. – 4. Forme di trasparenza. – 5. Conclusioni.

1. *Inquadramento*

Ultimamente, gli algoritmi sono ritenuti tra le principali fonti di rischio per la nostra libertà di autodeterminazione, per il diritto a rappresentare (senza deformazioni) il nostro "io" a livello digitale, a non essere sottoposti a decisioni totalmente automatizzate, ovvero ancora a non essere profilati; in effetti, questi "risolutori sistematici di problemi", alla base del c.d. *Machine Learning*, decidono il *ranking* di posizionamento nelle pagine dei motori di ricerca, sono in grado di prevedere le nostre scelte, di orientare le nostre preferenze, di stabilire se un criminale possa ancora ritenersi pericoloso o, meno.

Ma cos'è, esattamente, un algoritmo? In matematica ed informatica, un algoritmo viene definito come una sequenza finita di istruzioni con una semantica univoca e che possono essere eseguite da un computer al fine di risolvere una classe di problemi oppure eseguire una certa computazione. In maniera astratta, un algoritmo può essere visto come una funzione che prende un insieme di *input* (ad esempio due numeri) e li trasforma in un insieme di *output* (ad esempio il prodotto dei numeri). Perché un algoritmo può interessare la Pubblica Amministrazione (PA)? La risposta si trova nel fatto che la PA ha la possibilità di gestire grandi quantità di dati (*Big Data*) di varia natura (da quelli personali, a quelli relati-

* Avvocato e Direttore dell'Ufficio "Organizzazione e gestione della privacy" della Provincia autonoma di Trento.

** Ingegnere e Responsabile area Cybersecurity della Fondazione Bruno Kessler.

vi al territorio) e ha l'opportunità di utilizzare tali dati, processandoli tramite opportuni algoritmi, per snellire ed efficientare molti dei suoi processi, o ancora coinvolgere i cittadini nella definizione delle politiche per l'erogazione dei servizi.[1]

Come tutti gli strumenti, è necessario capire quali siano i punti di debolezza e quelli di forza degli algoritmi, al fine di sfruttare i secondi per migliorare la qualità dei servizi offerti dalla PA ed allo stesso tempo limitare l'impatto degli errori che possono risultare dal loro utilizzo come discriminazioni, o altri effetti negativi sui diritti e le libertà dei cittadini. A tale scopo è utile contrapporre due visioni per lo sviluppo degli algoritmi, che chiameremo rispettivamente classica e moderna. La prima si riferisce all'approccio classico, in cui un essere umano analizza un problema, o una classe, ne definisce un modello astratto (ovvero un modello che considera solo i parametri importanti per la soluzione) e, quindi, specifica un algoritmo (come detto un insieme di istruzioni eseguibili da un calcolatore) capace di risolverlo. La visione moderna, invece, è tipica degli algoritmi di *machine learning* e ha come caratteristica quella di utilizzare tecniche automatiche di apprendimento (*learning*), per derivare un modello astratto a partire da una grande quantità di dati che caratterizzano, o meno, soluzioni del problema da risolvere. Successivamente, il modello astratto viene utilizzato per risolvere nuove istanze del problema. La differenza principale tra i due approcci consiste nel fatto che l'intervento umano è preponderante nella visione classica, mentre è drasticamente ridotto nella visione moderna[2].

[1] Per una discussione approfondita su questo tema, si veda ad esempio, il recente (2019) OECD Working Paper 33, *A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance*. [https://www.sipotra.it/wp-content/uploads/2019/05/A-data-driven-public-sector-Enabling-the-strategic-use-of-data-for-productive-inclusive-and-trustworthy-governance.pdf]. Per un approfondimento sull'utilizzo dell'intelligenza artificiale nell'ambito delle azioni a tutela della salute pubblica durante l'emergenza Covid-19, vedi M. d'Agostino Panebianco, in *Covid-19: AI supports the fight, but reduces rights and freedoms*, Ordine internazionale e diritti umani, anno 2020.

[2] In tal caso, la sentenza n. 8472/2019 del Consiglio di Stato, richiamando il concetto di autonomia decisionale prevista nella Carta della Robotica approvata dal Parlamento europeo nel 2017, precisa come, allo stato attuale, le norme non siano ancora sufficienti ad attivare la responsabilità per i danni causati da un *robot*, in quanto non consentirebbero di determinare quale sia il soggetto su cui incombe la responsabilità («Occor-

Fiducia nell'algoritmizzazione della Pubblica Amministrazione: chimera o realtà?

Molto spesso il dialogo tra legali, da un lato, ed informatici-matematici, dall'altro, si rivela complesso, disallineato, o addirittura quasi impossibile per un linguaggio estremamente tecnico, di difficile traduzione per entrambi gli interlocutori, oltre che per fondamenti e principi del tutto differenti, che impediscono di conciliare i rispettivi punti di vista. Eppure, in ambito di protezione dei dati personali, si è oramai giunti alla necessità di una costante interazione tra i due approcci, per ambire alle migliori soluzioni in termini di efficacia ed efficienza, anche in termini di adeguamento al progresso tecnologico, compatibilmente con un principio di contenimento dei costi a carico del Titolare (artt. 25 e 32 del GDPR).

Nel presente saggio, gli autori si confrontano sul tema degli algoritmi ideati e/o utilizzati dalla PA per assumere decisioni nei confronti dei cittadini, alternandosi nell'esposizione delle rispettive convinzioni, talvolta anche esprimendo le proprie perplessità verso la tesi dell'interlocutore, ma sempre nel rispetto reciproco, in vista di un contemperamento, cioè alla ricerca di un compromesso tra due impostazioni e prospettive egualmente meritevoli: da un lato gli obblighi giuridici di trasparenza dell'azione amministrativa e, di conseguenza, dei relativi algoritmi, dall'altra la difficoltà intrinseca di produrre un'effettiva, oggettiva ed indiscutibile spiegazione matematica. Il quesito che ci si pone, in estrema sintesi, è: la pubblica amministrazione può utilizzare gli algoritmi nell'esercizio del proprio potere decisionale, essendo in grado di renderne trasparente la relativa logica e, quindi, di dimostrarne la coerenza con gli obiettivi pubblici prefissati, nonché l'assenza di errori e discriminazioni?

Machine Learning Algorithms and Public Administration: the Need for Reconciling Transparency with Efficiency

As AI and digital technology permeate more of our lives, they increasingly becomes the source of legally significant events. This means that those who study and/or practice Law increasingly need to understand the digital context. At the same time, those who study Computer Science and/or develop software increasingly need to understand potential legal consequences of design choices. This situation literally cries for an interdisciplinary approach to elaborate the many aspects of today and future Information and Communication Technology (ICT) systems. For this, a common language seems much needed to facilitate the transfer of problems, solutions, and concepts from Law to Computer Science and viceversa. To make the common language truly exploitable by experts in the two fields and foster mutual understanding, both lawyers and computer scientists need to develop an appreciation of the way in which they typically approach problems, with very different analytic tools. Reconciling the two views seems particularly urgent in the context of data protection to significantly limit the potential negative impacts on the rights and freedom of end users of ICT systems while meeting budget constraints as mandated by the GDPR (Art. 25 and 32).
This paper is an attempt to follow the path of a closer collaboration between Law and Computer Science on the problems posed by the use of Machine Learning algorithms in procedures adopted by the Public Administration. Indeed, one of the author is a lawyer (with a focus on data protection and privacy) and the other one is a Computer Science Engineer (with a focus on Cyber Security). The main focus of the discussion is in understanding the impact on citizens when the Public Administration adopts partially or fully automated decision processes. The goal of the discussion is to reach the "best" possible trade-off between, on the one hand, the need of administrative transparency, deriving from current regulations, that requires transparency of the algorithms used in any administrative process and, on the other hand, the intrinsic technical difficulties to explain the most efficient (in terms of scalability, performance, and precision) machine learning algorithms currently available. In particular, the authors attempt to provide a first answer to the following (crucial) question: can the Public Administration use algorithms for taking decisions in an more efficient way while being able to (i) motivate how such decisions have been taken, (ii) show that the process satisfies the predefined goals, and (iii) prove absence of bias and discrimination?

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 25-32

Uno sguardo critico sul *RenAIssance*

Nicola Busto*

Indice: 1. *Robota* e *RenAIssance*. – 2. La qualità del lavoro al tempo dell'IA. – 3. *Mechanical Turk*, un caso paradigmatico. – 4. Gli esseri umani al servizio delle macchine. – 5. Conclusioni.

1. Robota *e* RenAIssance

La parola "Robot" compare per la prima volta nel 1921 nel dramma utopico fantascientifico "R.U.R" (acronimo di "Rossumovi univerzální roboti") dell'autore ceco Karel Čapek[1].

Il neologismo, destinato ad una straordinaria fortuna in tutte le lingue, rimanda a "robota", "lavoro" in ceco. La trama della pièce teatrale si snoda a partire dal progetto della Rossumovi univerzální roboti, fabbrica in cui vengono creati esseri artificiali per sostituire gli uomini nello svolgimento ogni genere di robota.

L'utopia di liberare gli uomini dalla schiavitù del lavoro, consentendo loro di "vivere solo per perfezionarsi"[2] (che condurrà, nell'invenzione letteraria di Čapek, ad esiti catastrofici), sembra ancor oggi riverberarsi nel dibattito globale sulla intelligenza artificiale[3] e – parrebbe a chi scrive – in Italia riecheggia, tra gli altri[4], nel lavoro "Proposte per una strategia italiana per l'intelligenza artificiale"[5].

* Avvocato, attualmente *Contract Manager* nel settore consulenziale e tecnologico. Le opinioni espresse nel presente articolo sono a titolo puramente personale.

[1] Cfr. R.U.R. https://it.wikipedia.org/wiki/R.U.R. (25 maggio 2020).

[2] Cfr. A. Caronia, "L'uomo artificiale", «Burattini» n. 7, marzo 1986; n. 8, giugno 1986; n. 9, settembre 1986; n. 10-11, dicembre 1987 disponibile presso https://www.academia.edu/344486/Luomo_artificiale._Breve_storia_dei_doppi_umani_tecnologizzati_dal_mito_al_cyborg?email_work_card=title (25 maggio 2020).

[3] Cfr. G. Tett, I lavoratori e le macchine possono convivere, Internazionale n. 1337, 19 dicembre 2019.

[4] Cfr. *Ex multis*, P. Benanti, "RenAIssance Roma Call for AI Ethics", 4 marzo 2020, https://www.paolobenanti.com/post/renaissance-roma-call-for-ai-ethics (25 maggio 2020).

[5] Cfr. Gruppo di Esperti MISE sull'Intelligenza Artificiale, Verso una RenAIssance, "Proposte per una Strategia Italiana per l'Intelligenza Artificiale", luglio 2019, dispo-

In questo documento gli esperti del Ministero dello Sviluppo Economico[6] tratteggiano questa tecnologia come un'opportunità per inaugurare un nuovo Rinascimento (RenAIssance) economico, sociale e ambientale in cui:

«Proprio come il Rinascimento della metà del XIV secolo segna la scoperta di un nuovo modo di concepire il mondo, che pone al centro l'uomo con i suoi bisogni, le sue pulsioni e le sue sofferenze […] il RenAIssance […] potrebbe essere ispirato dal bisogno di definire un nuovo rapporto tra uomo e macchina, nel quale la tecnologia aumenta le capacità umane, e diviene strumento fondamentale per la scrittura di un nuovo contratto sociale, orientato verso lo sviluppo sostenibile».[7]

Perché ciò avvenga, avvisano gli esperti ponendosi in linea con le indicazioni ministeriali, l'avvento della IA dovrà essere governato da politiche "antropocentriche"[8], che ne consentano uno sviluppo complemen-

nibile presso https://www.mise.gov.it/images/stories/documenti/Proposte-per-una-strategia-italiana-2019.pdf (25 maggio 2020).

[6] Nel settembre del 2018, il Ministero dello Sviluppo Economico ha pubblicato un avviso per la selezione di 30 esperti provenienti dal mondo delle imprese, dalle istituzioni e dalla società civile, per affiancare tre membri del Ministero nel compito di elaborare una strategia nazionale sull'intelligenza artificiale. L'avviso pubblicato dal Ministero sottolineava che "lo sviluppo di sistemi di IA deve vedere l'uomo al centro in una sempre più complessa interazione con macchine intelligenti, e queste indefettibilmente devono essere in grado di spiegare le decisioni assunte sulla base degli algoritmi utilizzati. Dovrà dunque essere promosso un approccio 'human centric', che ponga al centro dello sviluppo dell'IA la persona e mitighi ogni possibile impatto sulla tenuta sociale e occupazionale, per un'armoniosa integrazione tra tecnologie IA, lavoratori e cittadini".

Cfr. Ministero dello Sviluppo Economico Direzione Generale per la Politica Industriale, la Competitività e le Piccole e Medie Imprese, Avviso pubblico per la manifestazione d'interesse per la selezione di 30 componenti del gruppo di esperti di alto livello per l'elaborazione della strategia nazionale sull'intelligenza artificiale, 14 settembre 2018, disponibile presso https://www.mise.gov.it/images/stories/documenti/Avviso%20manifestazione%20interesse.pdf (25 maggio 2020).

[7] Cfr. Gruppo di Esperti MISE sull'Intelligenza Artificiale, op. cit., par. Introduzione, p. 6.

[8] *Ivi*, p. 30 e 79. Tale visione, ispirata a quella della Commissione Europea e rinvenibile tra gli altri nelle "Ethic Guidelines for Trustworthy AI" dell'estate del 2018 e dal più recente "Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia", implica, tra gli altri, il rispetto dei seguenti principi:

Che l'IA sia in linea con la legislazione esistente e con i diritti fondamentali;

Che vengano incentivate forme di IA che aumentano l'intelligenza, la produttività e la creatività umana, anziché sostituirle;

Che l'IA rispetti pienamente l'integrità personale dell'individuo.

Uno sguardo critico sul RenAIssance

Secondo gli esperti del Ministero dello Sviluppo Economico italiano le tecnologie riconducibili all'intelligenza artificiale possono contribuire ad un nuovo Rinascimento (RenAIssance) nazionale.
Un contributo fondamentale al conseguimento di questo traguardo dovrà venire dalla creazione di politiche "antropocentriche" che dirigano lo sviluppo tecnologico in direzione complementare e funzionale all'intelligenza umana.
In assenza di questa azione di governo, le molteplici applicazioni dell'intelligenza artificiale, da opportunità, potrebbero trasformarsi in altrettanti rischi per la società; non ultimo il rischio di discriminazione lavorativa.
Partendo da questo assunto, il presente lavoro intende porre in luce come – quantomeno con riferimento alle interconnessioni tra Intelligenza artificiale e gig economy – la discriminazione lavorativa non costituisca un rischio futuro, ma un problema già oggi in grado di minare le basi etico/politiche del RenAIssance.

A critical look at RenAIssance

According to the Italian Ministry of Economic Development (MISE) experts, the artificial intelligence technologies can contribute to a new national Renaissance (RenAIssance).
A fundamental contribution to the achievement of this goal must come from the creation of "human centric" policies that direct technological development in order to complement and support the human intelligence.
A lack of governance can transform the multiple applications of artificial intelligence, from opportunities to risks for society; not least the risk of work discrimination.
Starting from this assumption, the present work intends to highlight how – at least with reference to the interconnections between Artificial Intelligence and gig economy – work discrimination does not constitute a future risk, but a problem already undermining the ethical / political foundations of the RenAIssance.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 33-48

Principio di neutralità tecnologica e progettazione dei sistemi informatici della pubblica amministrazione

Gherardo Carullo[*]

Indice: 1. Introduzione: il duplice problema della scelta dei mezzi e dell'inserimento di questi nella struttura del procedimento. − 2. La rilevanza dei costi di uscita nell'acquisizione dei mezzi digitali: il problema del *lock-in*. − 3. I criteri per la valutazione comparativa delle soluzioni tecnologiche e relativi oneri per l'amministrazione. − 4. La progettazione mediante affidamento esterno quale strumento di selezione e strutturazione delle tecnologie. − 5. La valorizzazione dei criteri di selezione dei sistemi informatici pubblici nella valutazione tecnico-economica delle offerte.

1. *Introduzione: il duplice problema della scelta dei mezzi e dell'inserimento di questi nella struttura del procedimento*

Gli strumenti digitali sono in misura crescente alla base dei procedimenti amministrativi e dell'azione amministrativa[1]. Tale fenomeno impone alle amministrazioni di dotarsi delle soluzioni informatiche più opportune rispetto alle proprie attribuzioni onde sfruttare al meglio le possibilità di efficientamento rese possibili dalle moderne tecnologie dell'informazione e della comunicazione (ICT)[2].

[*] Ricercatore (lett. b) nell'Università degli Studi di Milano, abilitato allo svolgimento delle funzioni di Professore di II fascia di Diritto Amministrativo, Dottore di ricerca in Diritto Amministrativo nella medesima Università, LLM al King's College di Londra.

[1] Sottolineava tale fenomeno già F. Benvenuti, *Il nuovo cittadino*, in *Scritti giuridici*, vol. I, Vita e Pensiero, 2006, p. 937 (opera pubblicata nel 1994, Venezia).

[2] *Ex multis* cfr. quanto in ultimo esposto da D.U. Galetta, "La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?", in «Ciberspazio e Diritto», 3, 2018; sul punto v. anche i contributi in S. Civitarese Matteucci, L. Torchia (a cura di), *A 150 anni dall'unificazione amministrativa italiana. La tecnificazione*, vol. IV, Firenze, Firenze University Press, 2017; J.E.J. Prins, M.M. Eifert, C. Girot, M. Groothuis, W.J.M. Voermans (a cura di),

Rispetto al contesto cartaceo, nel quale i processi produttivi potevano basarsi su prassi consolidate, l'«*attività di organizzazione*»[3] volta alla selezione delle ICT, anche in ragione della velocità del progresso tecnologico, può risultare particolarmente complessa in ragione delle molteplici variabili da considerare[4]. Tra queste, occorre qui sottolineare che la scelta degli strumenti digitali da acquisire presuppone sia l'individuazione delle soluzioni tecnologiche in sé considerate – quindi l'*hardware* e/o il *software* da acquisire –, sia l'inquadramento e la collocazione di dette soluzioni nell'ambito dei processi di lavoro dell'amministrazione[5].

Sotto il primo profilo si tratta di capire in concreto quali tecnologie informatiche siano effettivamente disponibili, quindi quali di queste possano essere implementate nelle strutture pubbliche e come le stesse possano essere acquisite, se ad esempio in autoproduzione, ovvero tramite fornitura da parte di terzi.

Il secondo profilo, ossia l'inquadramento e la collocazione delle soluzioni informatiche nell'ambito dei processi di lavoro, risulta strettamente connesso alla circostanza per cui l'azione amministrativa «*si esplica normalmente attraverso lo svolgimento di sequenze ordinate di atti e compor-*

E-Government and its Implications for Administrative Law: Regulatory Initiatives in France, Germany, Norway and the United States, TMC Asser Press, The Hague, 2002, p. 7.

[3] L'espressione è di M. Nigro, *Studi sulla funzione organizzatrice della Pubblica Amministrazione*, Giuffrè, Milano, 1966, p. 131.

[4] Nella letteratura tecnico-scientifica si trovano numerosi contributi che affrontano il problema, v. ad esempio S. Pant, T. Ravichandran, "A framework for information systems planning for e-business", in «Logistics Information Mngt», vol. 14, 1/2, 2001, pp. 85 e ss. «*while it is important for organizations to carefully plan for and architect ebusiness systems, none of the existing information systems planning models is adequate for the task. An e-business architecture planning model is developed by identifying 12 generic e-business models and three axes on which drivers of the information architecture needs of e-business firms fall. Sowa and Zachman's information architecture is augmented to further facilitate e-business information systems architecture planning*»,(v. anche M.P.C. Weijnen, P.M. Herder, I. Bouwmans, *Designing complex systems: A contradiction in terms*, in M. Eekhout; R. Visser; T. Tomiyama (a cura di), *Delft Science in Design 2, A Congress on Interdisciplinary Design*, vol. 3, Amsterdam, IOS Press, A 2008.

[5] Nell'ambito del management aziendale si è infatti sottolineato che una delle sfide principali «*è la costruzione di sistemi in grado di rispondere a interessi specifici interni all'azienda ma che nel contempo possano essere integrati in modo da fornire informazioni a tutta l'impresa*», K.C. Laudon, J.P. Laudon, *Management dei sistemi informativi*, II Ed., Milano, Pearson Italia S.p.a., 2006, p. 75.

Principio di neutralità tecnologica e progettazione dei sistemi informatici della pubblica amministrazione

L'acquisizione degli strumenti digitali necessari al funzionamento ed al supporto delle attività delle pubbliche amministrazioni introduce nuove variabili a partire dal momento stesso di individuazione dei mezzi a cui fare ricorso. La scelta verso determinate soluzioni esclude il ricorso ad altre, pur ove tecnicamente equipollenti, e può vincolare in modo sostanziale le opzioni a valle. Per far fronte a tali questioni il legislatore ha indicato una serie di criteri e princìpi per lo sviluppo, l'acquisizione ed il riuso di sistemi informatici nelle pubbliche amministrazioni. Tali criteri, tuttavia, non appaiono esaustivi delle esigenze da soddisfare, specie in rapporto alla definizione delle linee strategiche di sviluppo ed in funzione della programmazione di lungo periodo. L'articolo evidenzia tuttavia alcune criticità dell'attuale sistema, soprattutto per quanto riguarda il coordinamento tra le amministrazioni e in relazione alle garanzie di indipendenza di alcuni organi tecnici chiave. L'Autore propone perciò il ricorso agli strumenti di cui al Codice dei Contratti Pubblici per l'ideazione e la progettazione dei sistemi informatici delle amministrazioni.

Principle of technological neutrality and design of public administration IT systems

The acquisition of the digital tools necessary for the functioning and support of the activities of public administrations introduces new variables starting from the very moment of identifying the means to be used. The choice towards certain solutions excludes the use of others, even if technically equivalent, and can substantially constrain the downstream options. To deal with these issues, the legislator has indicated a series of criteria and principles for the development, acquisition and reuse of IT systems in public administrations. However, these criteria do not appear to be exhaustive of the needs to be met, especially in relation to the definition of the strategic lines of development and in function of the long-term planning. However, the article highlights some critical aspects of the current system, especially as regards coordination between administrations and in relation to the guarantees of independence of some key technical bodies. The author therefore proposes the use of the tools of public procurement for the conception and design of the IT systems of administrations.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 49-67

Il ruolo dei sistemi di *machine learning* nell'integrazione dei contratti incompleti: per un'applicazione alle clausole di *best efforts* nei contratti di licenza

Giuseppina D'Auria*

Indice: 1. Introduzione. – 2. Le clausole di *best efforts* nei contratti di licenza. – 3. Fenomenologia dei contratti di licenza. – 3.1. Peculiarità dei contratti di licenza. – 3.1.1. Durata. – 3.1.2. Complessità e incertezza intrinseche. – 3.1.3. Relazionalità. – 3.1.4. Investimenti specifici. – 4. L'incompletezza come necessità: la razionalità limitata. 5. L'incompletezza come scelta. – 6. I rischi endogeni: *moral hazard*. – 6.1. Il rischio di *hold-up*. – 7. I rischi esogeni: le sopravvenienze. – 8. I sistemi di *machine learning* come strumento di gestione dell'incompletezza contrattuale. – 8.1. Opportunità e criticità applicative. – 9. Conclusioni.

1. *Introduzione*

L'ordinamento giuridico garantisce e tutela l'autonomia negoziale, assicurando alle parti la libertà di disciplinare l'assetto di interessi che esse ritengano più adeguato alle loro esigenze. Esistono, tuttavia, casi per i quali non è possibile (o è molto improbabile) regolare nel dettaglio tutti gli aspetti del rapporto giuridico: l'informazione relativa a tali aspetti è troppo costosa o, semplicemente, non è nella disponibilità dei contraenti.

I costi di una negoziazione portata all'estremo, che contempli tutti gli stati futuri potenzialmente rilevanti e il calcolo del loro risultato efficiente, possono superare di gran lunga il ritorno atteso dalle parti. Poste di fronte a ineludibili aspetti di incertezza, le parti si vedono costrette a formulare clausole estremamente vaghe o, in estrema ipotesi, a rinunciare a inserirle nel contratto, rendendolo così fondamentalmente incompleto.

* Avvocato del Foro di Milano.

Per determinati contesti socioeconomici, l'obiettivo della contrattazione "completa" non è raggiungibile, poiché l'incertezza è un aspetto connaturale alla tipologia di contratti che vi si stipulano: appartengono sicuramente a tale ultima categoria i contratti di licenza esclusiva di brevetto. Per essi, i costi di transazione sono incrementati dalla durata (mediamente estesa), dalla complessità e dall'incertezza del mercato di riferimento, dal contesto relazionale e dalla presenza di investimenti specifici.

Nel presente lavoro[1] verranno analizzate, con specifico riferimento alle clausole di *best efforts* contenute nei contratti di licenza, le cause dall'incompletezza contrattuale (paragrafi 3, 4 e 5) e i rischi ai quali si espongono le parti in assenza di opportune tutele (paragrafi 6 e 7).

Un'ultima riflessione è dedicata alle nuove soluzioni prospettabili rispetto al tema dell'incompletezza contrattuale: in alternativa ai meccanismi contrattuali o istituzionali elaborati dalla teoria economica[2] e da quella giuridica[3] con l'obiettivo di prevenire i comportamenti opportunistici, verranno analizzate le conseguenze derivanti dall'eventuale impiego dei sistemi di *machine learning* (paragrafo 8).

2. *Le clausole di* best efforts *nei contratti di licenza*

I contratti di licenza dei brevetti industriali – e, più in generale, i contratti di gestione dell'innovazione[4] – costituiscono uno dei tipi più esemplificativi di contratti conclusi in contesti altamente collaborativi. Essi pongono in essere una forma di disseminazione, in cui una parte (l'inventore) gode (di parte) dei proventi derivanti dalla commercializzazione di beni prodotti dall'altra (il licenziatario). Ciascun contraente è

[1] Il presente lavoro si fonda sull'analisi di contratti negoziati tra parti sofisticate, assumendo che esse abbiano un potere contrattuale (approssimativamente) identico e che siano assistite (per lo più) da consulenti legali nella negoziazione. I contratti con i consumatori sono stati esclusi dall'analisi.

[2] Cfr., per un'ampia analisi della contrattazione incompleta, A. Nicita, V. Scoppa, *Economia dei contratti*, Bologna, Carocci Editore, 2005.

[3] Cfr. diffusamente sul punto G. Bellantuono, *I contratti incompleti nel diritto e nell'economia*, Padova, Cedam, 2000; A. Fici, *Il contratto incompleto*, Torino, Giappichelli, 2005.

[4] Cfr. P. Aghion, J. Tirole, "The management of innovation", «The Quarterly Journal of Economics», vol. 109, n. 4, 1994, pp. 1185-1209.

Il ruolo dei sistemi di machine learning *nell'integrazione dei contratti incompleti: per un'applicazione alle clausole di* best efforts *nei contratti di licenza*

I contratti di licenza esclusiva di brevetto sono, per loro natura, contratti incompleti, dal momento che alcune loro caratteristiche (durata, razionalità limitata e incertezza intrinseca al mercato di riferimento, contesto relazionale, presenza di investimenti specifici) rendono particolarmente elevati i costi di transazione.
Con specifico riferimento alle clausole di *best efforts* presenti nei contratti di licenza, il presente lavoro analizza alcune delle cause che sono alla base dell'incompletezza contrattuale, per poi evidenziare i rischi – sia interni sia esterni al rapporto contrattuale – ai quali si espongono le parti in assenza di opportune tutele.
Nel modello proposto, a certe condizioni, le tecniche di sfruttamento computazionale dei dati potrebbero rappresentare un utile strumento per stabilire *ex ante* quali prestazioni siano esigibili dalla parte di volta in volta obbligata ai *best efforts* affinché sia conseguita la massima utilità congiunta delle parti.
L'eventuale adozione di sistemi di questo tipo pone il giurista di fronte a diverse sfide: a parte l'ovvia difficoltà di garantire l'attendibilità dei dati, sussiste anche il rischio che l'innovazione in ambito contrattuale sia frenata dall'uso di *data set* che rispecchiano lo *status quo* delle negoziazioni.

Machine learning's role in filling the gaps of incomplete contracts: an application to the "best efforts" clauses in licensing

Exclusive patent licencing agreements are incomplete contracts by nature, since some of their features (duration, limited rationality, technological uncertainty, relational contracting, idiosyncratic investments) make transaction costs particularly high.
With reference to 'best efforts' clauses in licencing, this paper focuses on some of the reasons underlying the contractual incompleteness, and then highlights the internal and external risks the parties without an adequate protection are exposed to.
Under certain conditions, machine learning techniques could become a useful tool to set forth the best effort obligations to maximize the joint surplus of the parties.
The possible deployment of such systems presents lawyers with several challenges: besides the difficulty of ensuring the data correctness, there is also the risk that contractual innovation will be hampered by the use of data sets that reflect the *status quo* of negotiations.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 69-84

Intelligenza Artificiale e amministrazioni pubbliche: tra passato e presente

Francesco Romano*

Indice: 1. Introduzione. – 2. AI e PA: questioni tecniche, etiche e giuridiche. – 3. AI e servizi della PA. – 4. AI e PA questioni culturali. – 5. Soluzioni possibili.

1. *Introduzione*

Di informatizzazione della pubblica amministrazione e anche di applicazioni di intelligenza artificiale[1] (o di intelligenza aumentata) per le amministrazioni pubbliche e più in generale per l'automazione del ragionamento giuridico si parla da molti anni.

Attualmente, le iniziative nel settore si moltiplicano, basti osservare la vasta produzione scientifica, i molti convegni, corsi universitari, progetti e proposte che anche le Agenzie nazionali preposte all'informatizzazione del settore pubblico stanno avanzando[2].

Abbiamo verificato nella banca dati DoGI[3] la presenza di articoli e saggi della dottrina su materie quali sistemi esperti o il rapporto tra ragionamento giuridico e informatica trovando un'ampia e variegata casisti-

* Francesco Romano è ricercatore all'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR. Questo saggio è la sintesi della relazione svolta a ICON·S Italian Chapter, Seconda Conferenza *Le nuove tecnologie e il futuro del diritto pubblico*, Firenze, 22-23 novembre 2019, nell'ambito della tavola rotonda intitolata *L'intelligenza artificiale "predittiva" in ambito pubblico: norme e casi*.

[1] L'intelligenza artificiale era definita da Sartor come la «scienza intesa a sviluppare modelli computazionali del comportamento intelligente, e quindi a far sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo». G. Sartor, *Intelligenza artificiale e diritto: un'introduzione*, Milano, Giuffrè, 1996, p. 6.

[2] Si pensi all'istituzione della Task Force Intelligenza Artificiale – IA-Gov. Vedi tutti i progetti e le attività compreso il *Libro Bianco sull'IA al servizio del cittadino* sul sito web https://ia.italia.it/materiali/.

[3] DoGi è una banca dati di riferimenti bibliografici di articoli pubblicati su riviste giuridiche italiane (vedi http://www.ittig.cnr.it/dogi/).

ca di articoli e saggi che prospettavano l'uso di tali tecnologie anche nel campo della pubblica amministrazione già sul finire degli anni Settanta del secolo scorso (in nota si evidenzia una bibliografia ragionata sul tema che va dal 1978 al 2015)[4].

[4] Si vedano (in ordine dal più recente al più risalente) ad esempio G.M. Losano, "La macchina analitica di Babbage: un fossile che viene dal futuro", «Il Diritto dell'informazione e dell'informatica», fasc. 1, 2015, pp. 1-42; C. Castelfranchi, "Cognitivizzare le norme. Internalizzazione ed elaborazione dei costrutti mentali normativi", «Informatica e diritto», fasc. 1, 2013, pp. 75-98; U. Bechini, D. Gassen, "Firme elettroniche a valore legale internazionale: un nuovo approccio per migliorare l'interoperatività", «Studi e materiali», fasc. 4, 2009, pp. 1589-1609; G. Bucci, V. Sandrucci, E. Vicario, "Potenzialità del paradigma ontologico nello sviluppo di applicazioni di e-Government", «Informatica e diritto», fasc. 1-2, 2008, pp. 279-287; G. Sartor, "Sistemi basati sulla conoscenza giuridica e servizi pubblici", «Informatica e diritto», fasc. 1-2, 2008, pp. 463-476; A. Viterbo, A. Codignola, "I 70 anni del Manifesto dell'intelligenza artificiale", «Il Diritto dell'informazione e dell'informatica», fasc. 4-5, 2007, pp. 725-740; P. L. Lucatuorto, "Intelligenza artificiale e diritto: le applicazioni giuridiche dei sistemi esperti", «Ciberspazio e diritto», fasc. 2, 2006, pp. 219-241; F. Romano, "La gestione delle informazioni nel progetto TeleP@B: progettazione di strumenti per l'accesso semplificato ai documenti del bilancio", «Informatica e diritto», fasc. 1, 2006; E. Belisario, "La disponibilità dei dati delle pubbliche amministrazioni nel Codice dell'amministrazione digitale", «Informatica e diritto», fasc. 1-2, 2005, pp. 167-181; E. Fameli, "SIAM/Lav: un "sistema intelligente integrato" come supporto alla consulenza e alla decisione nell'applicazione delle clausole generali di correttezza e di buona fede alle procedure concorsuali private", «Informatica e diritto», fasc. 1-2, 2004, pp. 177-258; G. Duni, "L'autenticità degli atti in forma elettronica", «Rivista giuridica sarda», fasc. 1, pt. 2, 2001, pp. 295-298; S. Stefanelli, "Diritto e Intelligenza artificiale. Alcune riflessioni nell'ambito del paradigma argomentativo", «Informatica e diritto», fasc. 1, 1999, pp. 7-22; G. Terracciano, "L'applicazione in campo giuridico delle reti neurali artificiali. Il programma "GiuriNet"", «I tribunali amministrativi regionali», fasc. 12, pt. 2, 1998, pp. 497-509; A. Liserre, "Sul rapporto fra automazione e diritto: l'avvento del documento elettronico", «Rivista del notariato», fasc. 5, pt. 1, 1998, pp. 809-816; V. Buscema, "Data base structured query language e reti neutrali: un felice connubio", «Il foro amministrativo», fasc. 1, pt. 2, 1997, pp. 376-379; D. Intrigila, M. Cianci, P. Damiani, P. Di Salvatore, "Modelli computazionali di sistemi su larga scala di norme giuridiche", «Informatica e diritto», fasc. 1, 1997, pp. 7-35; E. Fameli, "Modelli di "sistemi esperti integrati" nel diritto: problemi di configurazione e metodologia di sviluppo", «Informatica e diritto», fasc. 1, 1995, pp. 191-239; L. Lombardi Vallauri, "Verso un sistema esperto giuridico integrale", «Jus», fasc. 2, 1995, pp. 207-225; E. Barucci, L. Landi, "Un modello di intelligenza artificiale per la previsione dell'asta dei Bot", in «Bancaria», fasc. 2, 1994, pp. 66-74; M. Flores, "I sistemi informatici di supporto alla decisione", «Rivista giuridica della scuola», fasc. 3, pt. 1, 1994, pp. 459-464; G. Quirchmayr, R. Traunmueller, W. Bauer, "Hyper Reasoner: un esempio di integrazione tra ipermedia e tecnologia dei sistemi esperti", «Informatica e diritto», fasc. 2, 1994, pp. 261-272; V. Buscema, "Discrezionalità amministrativa e reti neurali artificiali", «Il foro amministrativo», fasc. 2-3, pt.

Intelligenza Artificiale e amministrazioni pubbliche: tra passato e presente

Nel presente contributo cercheremo di verificare quali fossero le questioni che già dagli anni Ottanta si ponevano relativamente all'uso dei sistemi di IA nella pubblica amministrazione. Vogliamo verificare se le criticità che si prospettavano siano state in tutto o in parte risolte o se siano ancora attuali, anche solo relativamente a singoli aspetti o temi. Vedremo poi alcuni fra i temi affrontati nel Libro Bianco sull'IA al servizio del cittadino, curato da AgID, per verificare come l'intelligenza artificiale possa effettivamente impattare sui servizi che la PA deve erogare a cittadini ed imprese, ciò soprattutto al fine di attuare con concretezza quel principio di cittadinanza digitale da anni enunciato.

Artificial Intelligence and public administrations: between past and present

In this paper we will try to verify what the issues that already arose in the 1980s regarding the use of AI systems in public administration. We want to check whether the critical issues that have emerged have been fully or partially solved or whether they are still current, even if only in relation to individual aspects or themes. We will then see some of the issues addressed in the White Paper on AI at the service of the citizen, edited by AgID, to verify how artificial intelligence can actually impact on the services that the PA must provide to citizens and firms, especially in order to implement concretely that principle of digital citizenship that has been enunciated for years.

GDPR, Sicurezza e Protezione dei Dati

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 87-102

GDPR e dati personali nei rapporti B2B

Gabriella Caiazza*

Indice: 1. Applicabilità del GDPR ai dati degli addetti nei rapporti B2B. – 2. Trattamenti comunemente ricorrenti. – 3. Diritti dell'interessato. – 4. Esercizio dei diritti dell'interessato. – 5. Difficoltà di applicazione. – 6. Clausola contrattuale privacy B2B. – 7. Problematiche applicative. – 8. Conclusione.

La normativa europea sulla protezione dei dati[1] (in seguito GDPR o Regolamento) è stata emanata per la protezione e la libera circolazione dei dati personali, che sono tutte le informazioni relative a una persona fisica identificata o identificabile (interessato). L'Art. 5 GDPR prevede che ogni trattamento di dati personali debba essere lecito, corretto e trasparente.

I destinatari del GDPR sono principalmente persone giuridiche pubbliche e private che trattano dati personali in qualità di titolari del trattamento.

Il titolare del trattamento dei dati personali è il soggetto che decide le finalità e le modalità del trattamento dei dati personali.

Non c'è dubbio che un datore di lavoro, in qualità di titolare del trattamento, sia soggetto al GDPR per il trattamento dei dati personali dei propri dipendenti e collaboratori. Una questione diversa è quando lo stesso titolare tratta i dati personali dei dipendenti dei suoi partner commerciali (ad esempio clienti e fornitori) nell'ambito delle sue relazioni contrattuali B2B, quindi l'oggetto di questo articolo.

* Law graduate svedese-italiana presso University of Essex, qualificata Data Protection Officer, attualmente in training per potersi qualificare come Solicitor nel Regno Unito.

[1] Regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (General Data Protection Regulation).

Esaminando i considerando del Regolamento, la protezione dei dati sembra concentrarsi sui dati personali di consumatori, utenti e dipendenti.

Le parole '*employee*' (lavoratore dipendente) ed '*employment*' (rapporto di lavoro subordinato) sono menzionate oltre 20 volte nel GDPR, ma sempre per quanto riguarda il rapporto tra il datore di lavoro, come titolare del trattamento dei dati, ed il suo dipendente come interessato. Quando il titolare del trattamento dei dati personali è il datore di lavoro non vi è quindi alcun dubbio sulla protezione obbligatoria dei dati personali dei propri dipendenti in quanto interessati.

Quando il trattamento dei dati personali riguarda i dipendenti di un altro soggetto, ad esempio un partner commerciale nell'ambito dei rapporti contrattuali B2B, il titolare del trattamento non è il suo datore di lavoro, ma il cliente o il fornitore del suo datore di lavoro.

Tale situazione si verifica quotidianamente, ad esempio quando un datore di lavoro trasferisce dati personali dei propri dipendenti a un altro titolare del trattamento dei dati (ad esempio un cliente o un fornitore) comunicando i nomi e alcuni dati del proprio personale di vendita o di altri lavoratori per eseguire un servizio o fornire assistenza tecnica. Il destinatario delle comunicazioni, in qualità di titolare del trattamento dei dati, è tenuto a trattare tali dati personali in conformità al GDPR.

Ad oltre due anni di applicazione del GDPR, obbligatorio dal 25 maggio 2018, sembra che questo tipo di trattamento non sia sufficientemente preso in considerazione dai titolari del trattamento, che generalmente predispongono e forniscono informative privacy ai propri dipendenti,[2] candidati che inviano CV, collaboratori, clienti, potenziali clienti, utenti di siti web, destinatari di newsletter e altre persone fisiche, mentre i dipendenti che lavorano per un'azienda terza raramente ricevono le informazioni dalle imprese che intrattengono un rapporto contrattuale con il loro datore di lavoro.

[2] S. Stokes, "Data protection, information security, and cloud computing", «Compliance Officer Bulletin», 2019.

GDPR e dati personali nei rapporti B2B

I dati personali dei lavoratori circolano tra le imprese che intrattengono rapporti di affari.
La maggior parte delle offerte, degli ordini, delle vendite e delle vicende relative ai rapporti contrattuali sono comunicati da addetti che comunicano il proprio nome e vengono ricevuti da altrettanti addetti del destinatario. Le comunicazioni commerciali contengono dati personali che meritano la protezione prevista dal GDPR.
Le imprese non appaiono sensibilizzate su questo genere di trattamenti e sono ancora poche quelle che forniscono l'informativa obbligatoria agli addetti dei propri business partner.
L'adempimento a detto obbligo di informazione è particolarmente gravoso per i titolari che dovrebbero mappare i propri archivi, programmi CRM, banche dati, messaggi e-mail risalenti negli anni per individuare tutti i dati personali raccolti nei rapporti B2B e informare ciascun interessato del trattamento in corso.
Una soluzione viene proposta nel presente articolo sotto forma di clausola contrattuale che sia sufficiente ad evitare di inviare l'informativa a ciascun interessato che lavori per un'impresa che intrattiene rapporti d'affari con l'impresa titolare.

GDPR and the processing of personal data in B2B relationships

Personal data of workers circulates among enterprises doing business with each other.
Most offers, orders, sales and events relating to contracts are communicated by a given employee disclosing his or her name and received by recipient's employee. Business communications are filled with personal data deserving protection under the General Data Protection Regulation - GDPR.
Companies do not seem to focus on this kind of processing and still too few are providing the mandatory information to business partners' employees.
To comply with information obligation is a heavy burden for data controllers who should scan their archives, CRM programs, data bases, email messages of the past years to detect personal data in B2B relationships and inform each data subject of the processing ongoing.
A solution is proposed in this paper in the form of a contractual clause which should be sufficient to avoid sending the information to each data subject working for a company doing business with the data controller.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 103-122

Blockchain e le sue applicazioni forensi: uno studio sulla sicurezza

Michele Chierici*

Indice: 1. *Distributed Ledger Technology* e sue funzioni – 2. Validità giuridica – 3.1 Libertà delle prove – 3.2 Libera valutabilità – 4. CAD e eIDAS – 5. Certezza del DLT e ruolo della fiducia – 5.1 Funzionamento e sicurezza della blockchain – 5.1.1 *Preimage resistance* – 5.1.2 S*econd preimage resistance* – 5.1.3 *Collision resistance* – 5.2 Attacco al checkpoint – 5.3 Attacco del 51% – 5.4 *Collision attack* – 5.5 Attacco Eclipse – 6. Conclusioni.

1. Distributed Ledger Technology *e sue funzioni*

Oggigiorno si fa ampio uso di registri contabili per annotare avvenimenti fornendone una localizzazione temporale, detti registri per l'appunto riportano informazioni storiche, ossia già avvenute, delle quali vi è necessità di tenerne memoria.

Ponendo il caso di due soggetti, uno dotato di valuta e l'altro di beni di consumo, e che tra i due intercorra un rapporto continuativo di scambio beni-valuta, per sapere dopo un lasso di tempo se effettivamente vi sia stata parità tra quanto dato e quanto ricevuto, sarà sufficiente incrociare i dati dei due registri tenuti dalle parti[1]. In altre occasioni, viceversa è possibile che il registro sia unico e si trovi nelle mani di un terzo, come ad esempio i registri dello stato civile, che, a norma dell'art. 449 c.c., sono pubblici ma la loro tenuta viene demandata all'ufficiale di stato civile. L'art. 451 c.c. ci ricorda inoltre che detti registri hanno una particolare importanza poiché gli atti ivi contenuti fanno prova fino a querela di falso; ciò è alla base di quello che viene oggi definito come certezza del diritto, principio cardine dell'ordinamento che permette agli individui di agire e prevedere i risultati giuridici delle loro azioni.

* Università degli Studi di Parma.

[1] Questo procedimento viene detto *data reconciliation* e comporta l'attività di più soggetti (più è complessa la struttura organizzativa maggiore sarà il lavoro necessario per acquisire tutte le informazioni) nonché un ingente dispendio di tempo e risorse.

Sono varie le problematiche collegate alla scelta del tipo di registro, occorre pertanto, in primo luogo, predisporre un'analisi costi-benefici. Ad esempio, un *data reconciliation* effettuato su una vasta mole di informazioni contempla alti costi in termini di lavoro e tempo, proprio per questo motivo, a volte, viene preferito l'uso di registri condivisi (c.d. *shared ledgers*) nei quali gli operatori possono scrivere rispettando una serie di regole. Questo sistema basato sulla fiducia fa si che un operatore possa rinunciare alla tenuta del proprio registro[2] ed ottenere al contempo un risparmio sia in termini di costi di gestione che di *data reconciliation* (il quale diviene inutile poiché non vi è più una pluralità di registri). Tra i registri condivisi stanno prendendo piede i cosiddetti DLT (*distributed ledger technology*), ossia reti peer-to-peer rette dal sistema del consenso[3] per mezzo di un algoritmo che consente a ciascun utente di poter inserire i propri dati ma senza rinunciare al controllo effettuato da altri (evitando ad esempio i problemi di *double spending* nei quali un soggetto malintenzionato iscrive due volte la medesima somma a suo favore).

Si proseguirà con l'analizzare l'attitudine dei registri DLT, di cui i più famosi basati su architettura blockchain, ad essere utilizzati in àmbito forense[4], come prove di un procedimento giudiziario, e infine, se tali registri possano effettivamente fornire una prova attendibile del loro contenuto.

[2] Precisamente il registro è tenuto da tutti coloro che ne sono intenzionati, essendo digitale è possibile scaricarlo interamente sul proprio computer con un sacrificio di memoria minimo (si parla di pochi GB di memoria). Ciò non impedisce che viceversa si opti per l'assoluto abbandono del registro che rimarrà comunque nelle mani di una comunità garante delle operazioni. Avendo dimensioni così ridotte è anche possibile tenere l'intero registro sul proprio smartphone.

[3] A. Porat, A. Pratap, P. Shah, V. Adkar, *Blockchain consensus: an analysis of proof-of-work and its applications*, in http://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf (link verificato il 24/1/2019) il protocollo blockchain è basato su algoritmi Proof Of Works i quali sono accessibili senza limitazioni, differente è il caso delle blockchain private dove i partecipanti sono soggetti qualificati e selezionati il cui unico scopo è quello di validare le transazioni. Il Proof Of Work consiste nella controprestazione in «lavoro» da effettuarsi per ottenere il servizio e fintanto che non sarà risolto l'algoritmo non si potrà passare al blocco successivo. Il nodo che per primo risolve il calcolo trasmette agli altri nodi il messaggio, questi sono in grado di verificare rapidamente se l'operazione è corretta o se il primo nodo ha malintenzionatamente tentato di ingannarli.

[4] Così già avviene in Cina, alla Corte di Hangzhou, come riportato dalla prima e più grande agenzia di stampa cinese Xinhua, in http://www.xinhuanet.com/english/2018-12/08/c_137658750.htm

Blockchain e le sue applicazioni forensi: uno studio sulla sicurezza

Questo elaborato indaga sulla possibilità dell'utilizzo della blockchain in àmbito forense. Si tratta in primo luogo di capire se questa sia ammissibile all'interno di un procedimento ed in secondo luogo che valore possa avere. Data l'alta innovatività della tecnologia in questione non vi sono riferimenti normativi specifici, pertanto sarà necessario avvalersi dell'interpretazione di norme generiche già esistenti.

Blockchain and forensic applications: security study

This paper analyzes the possible applications of the blockchain in the judicial civil process. First of all, it is necessary to understand if the blockchain can be used and compare it with current legislation of the others proofs. There is no special regulation therefore the generic one must be interpreted. In the second hand, it will be necessary to qualify the blockchain and understand what probative value it has.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 123-169

Principi di sicurezza applicabili ai *cloud computing services*: GDPR, Direttiva NIS e PSD2 a confronto

Marco Tullio Giordano[*], Isabella Oldani[**], Massimo Simbula[***]

Indice: 1. Introduzione. – 2. I principi e le misure di sicurezza applicabili ai *cloud service providers*: l'approccio del GDPR. – 2.1. Misure tecniche e organizzative previste dal GDPR. – 2.2. I principi di sicurezza in relazione al trasferimento dei dati a paesi terzi. – 3. I principi e le misure di sicurezza applicabili ai *cloud service providers*: l'approccio della Direttiva NIS. – 4. I principi e le misure di sicurezza applicabili ai *cloud service providers*: l'approccio della PSD2. – 5. Le differenze e le sovrapposizioni tra gli obblighi previsti dal GDPR, dalla NIS e dalla PSD2. – 5.1. Le sovrapposizioni tra NIS e GDPR. – 5.2. Le sovrapposizioni tra PSD2 e GDPR. – 6. Conclusioni.

1. *Introduzione*

La protezione dei dati personali e, ancor più in generale, la sicurezza informatica sono diventati negli ultimi anni temi di importanza primaria sia a livello nazionale che a livello sovranazionale. Ciò è testimoniato dall'adozione (nel 2016) e successiva applicazione (nel 2018) di due normative comunitarie che hanno ridisegnato la cornice di riferimento per la protezione dei dati e per la sicurezza dei sistemi informativi: il Rego-

* Paragrafo 1 – paragrafo 2.1. – paragrafo 3. Avvocato in Milano, Si occupa di diritto penale, data protection e cybersecurity nella società dell'informazione. È Data Protection Officer e Lead Auditor certificato ISO/IEC 27001:2014 ed è fellow del Cloud Security Alliance – Italy Chapter.

** Paragrafo 1 – paragrafo 2.2. – paragrafo 5 (introduzione) e 5.1 – paragrafo 6. Avvocato presso il Foro di Milano, specializzata nella *compliance* in materia di protezione dei dati personali e coordinatrice delle attività di ricerca "Legal and Privacy in the Cloud" del Cloud Security Alliance – Italy Chapter.

*** Paragrafo 1 – paragrafo 4 – paragrafo 5.2. Avvocato in Cagliari, si occupa, tra le altre materie di interesse, di privacy e regulation del settore fintech. È stato fondatore dell'Associazione Copernicani e fa parte del comitato scientifico della Associazione Nazionale Protezione Dati.

lamento Generale sulla Protezione dei dati personali ("Regolamento" o "GDPR")[1] e la Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, meglio nota come Direttiva NIS (*Network and Information Security*).[2] In questo quadro normativo si inserisce anche la Direttiva 2015/2366/(UE)[3] sui servizi di pagamento prestati nel mercato interno europeo ("PSD2") che ha introdotto significative novità nel mondo dei pagamenti digitali.

I fornitori dei servizi *cloud* ("*cloud service providers*" o "CSPs") sono quindi stati "investiti" dal susseguirsi di novità normative e dal sovrapporsi di numerosi obblighi derivanti dalla spesso simultanea applicazione del GDPR, della Direttiva NIS e, talvolta, anche della PSD2. La sovrapposizione delle disposizioni prescritte da normative differenti può ingenerare confusione nella gestione degli obblighi da queste imposti. Fare chiarezza in questo contesto di incertezza risulta di essenziale importanza non solo per permettere una corretta gestione dei vari adempimenti ma anche per permettere ai destinatari di tali obblighi di sfruttare tali sovrapposizioni al fine di ottimizzare, invece che moltiplicare, i propri sforzi applicativi.

La presente ricerca si propone quindi di analizzare le prescrizioni contenute nel GDPR e nella Direttiva NIS in materia di sicurezza al fine di individuare: (1) le misure tecniche e organizzative che i fornitori di servizi *cloud* sono tenuti ad applicare e gli obblighi di notifica previsti dal Regolamento e dalla Direttiva; (2) le sovrapposizioni e, al contempo, (3) le differenze tra le prescrizioni in esame nel loro contenuto, nei loro presupposti applicativi, nei criteri e nei rischi sulla base dei quali l'adeguatezza delle misure di sicurezza deve essere valutata. Questa analisi sarà inoltre completata dall'esame dei corrispettivi obblighi imposti dalla PSD2.

[1] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[3] Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

Principi di sicurezza applicabili ai cloud computing services*: GDPR, Direttiva NIS e PSD2 a confronto*

La protezione dei dati personali e la sicurezza informatica sono diventati negli ultimi anni temi di importanza primaria come testimoniato dall'adozione (nel 2016) e successiva implementazione (nel 2018) di due normative comunitarie che hanno ridisegnato la cornice di riferimento in materia: il GDPR e la Direttiva NIS. In questo quadro normativo, si inserisce anche la Direttiva PSD2 che ha introdotto significative novità nel mondo dei pagamenti digitali. I fornitori di servizi *cloud* sono stati così "investiti" dal susseguirsi di novità normative e dal sovrapporsi di numerosi obblighi derivanti dalla spesso simultanea applicazione del GDPR, della Direttiva NIS e, talvolta, anche della PSD2. La presente ricerca si propone quindi di analizzare (1) le prescrizioni in materia di sicurezza che i fornitori di servizi *cloud* sono tenuti ad applicare ai sensi delle tre normative, (2) le sovrapposizioni e, al contempo (3) le differenze tra le prescrizioni in esame nel loro contenuto e nei loro presupposti applicativi.

Security principles applicable to cloud computing services: comparison between GDPR, NIS Directive and PSD2

In recent years, the protection of personal data and information security have become issues of primary importance as evidenced by the adoption (in 2016) and subsequent implementation (in 2018) of two EU laws that have reshaped the framework on the subject: the GDPR and the NIS Directive. The PSD2 Directive is also included in this regulatory framework since it has introduced significant novelties in the world of digital payments. Cloud service providers have hence found themselves subject to new regulations and, consequently, to a number of new overlapping obligations stemming from the often-simultaneous application of the GDPR, the NIS Directive and, sometimes, of the PSD2. The present research hence aims to analyze (1) the security obligations that the three laws in question impose on cloud service providers, (2) the overlapping points and, at the same time (3) the differences between such obligations in their content and scope of application.

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 171-181

Pandemia, emergenza e protezione dati personali negli ambienti di lavoro: verso la ripresa dell'attività produttiva

Chiara Ciccia Romito*

Indice: 1. Le fonti normative e i pareri delle Autorità Garanti. – 2. L'entrata in vigore del DPCM 11 marzo 2020 e il protocollo di attuazione. – 3. Le basi giuridiche del trattamento. – 4. Le misure necessarie per un trattamento a norma. – 5. Conclusioni.

1. *Le fonti normative e i pareri delle Autorità Garanti*

La confusione creata dalla situazione d'emergenza, prima dell'entrata in vigore del DPCM 11 marzo 2020[1] aveva introdotto nelle imprese e nelle organizzazioni l'erronea convinzione che la situazione d'emergenza giustificasse qualsiasi misura tesa a scongiurare l'evolversi della pandemia. Invero, ancora prima del *lockdown* si era introdotta la prassi di sottoporre i lavoratori alla misurazione della temperatura corporea o alla sottoscrizione di modelli auto-dichiarativi relativi non solo al proprio stato di salute, ma altresì a quello di famigliari e conoscenti con cui il lavoratore era entrato in contatto negli ultimi 14 giorni.

A tal uopo, la nostra Autorità Garante con Provvedimento del 2 marzo 2020 è intervenuta invitando i titolari del trattamento ad evitare pratiche "fai da te" ed attenersi alle solo indicazioni dettate dal Ministero della Salute.

* Avvocato in Modena, ha conseguito il perfezionamento in "Criminalità informatica ed investigazioni digitali". Collabora con la Cattedra di "Informatica Giuridica" dell'Università degli Studi di Milano come cultore della materia e Fellow Research dell'Information Society Law Center – ISLC dell'Università degli Studi di Milano.

[1] Cfr. Decreto del Presidente del Consiglio dei Ministri, recante ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale (GU Serie Generale n.64 del 11-03-2020).

Nell'ordinamento italiano, il datore di lavoro può venire a conoscenza delle condizioni di salute, ma solo nelle modalità definite dalla legge.

Invero, l'Art. 5 dello Statuto dei lavoratori[2] vieta gli accertamenti da parte del datore di lavoro e sulla base di quanto statuito dal D.lgs. 81/2008[3], tali accertamenti sono demandanti al medico competente.

Oltre ciò, la Circolare del 12.03.2013 emanata di concerto dal Ministero del Lavoro con il Ministero delle Politiche Sociali e della Salute avevano affrontato l'argomento in relazione al divieto di indagine clinica relativo alla sieropositività del dipendente. La Circolare in parola, specificava che nell'ambito della sorveglianza sanitaria, l'indagine relativa allo stato di salute del dipendente non può essere effettuata né come accertamento preventivo né in associazione a misure d'igiene e prevenzione.

Il Garante con l'intervento *de quo* ha ribadito la portata del principio, in attesa delle prescrizioni da parte del Governo, che successivamente ha emanato il DPCM 11 marzo 2020.

Sulla scorta della situazione di incertezza, sono intervenute, altresì, le Autorità Garanti europee cercando di interrompere il fenomeno di *self adjustment* negli ambienti di lavoro che stava caratterizzato la gestione dell'impresa in tutti i Paesi colpiti dalla pandemia.

Il Garante danese (DatatyIsinet) ha chiarito che, nell'ambito della situazione d'emergenza, il datore di lavoro può raccogliere informazioni solo in "larga misura", e quindi, trattare le sole informazioni generalizzate non attinenti lo stato di salute. Per il DatatyIsinet è possibile che il datore di lavoro venga a conoscenza del fatto che un dipendente sia rientrato da una cd zona a rischio, ma non è autorizzato a conoscere lo stato di salute del dipendente.

Il CNIL, Autorità Garante francese, ha confermato l'interpretazione del Garante italiano e danese, invitato i datori di lavoro ad astenersi da compiere attività di raccolta sistematica e generale circa i sintomi presentati dai dipendenti.

[2] Sono vietati accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente. Il controllo delle assenze per infermità può essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti, i quali sono tenuti a compierlo quando il datore di lavoro lo richieda. Il datore di lavoro ha facoltà di far controllare la idoneità fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico.

[3] Testo unico sulla salute e sicurezza del lavoro.

Pandemia, emergenza e protezione dati personali negli ambienti di lavoro: verso la ripresa dell'attività produttiva

Il quadro emerso dalla situazione della pandemia che ha colpito l'Europa comporta delle riflessioni che investono il delicato profilo dell'esigenza della protezione dei dati nell'ambito dell'attività di impresa unita alla necessità di ripresa economica.
Uno dei settori inevitabilmente coinvolti nella gestione della pandemia è quello relativo alla gestione dei dati dei lavoratori al fine di attuare le misure preventive anti-contagio obbligatorie in tutte le imprese ed organizzazioni in attuazione del DPCM 11 Marzo 2020. Lo stesso ha previsto misure volte a favorire la ripresa dell'attività economica attraverso il ripristino della produzione limitata all'osservanza di regole anti-contagio.
Il rispetto delle regole predisposte al fine di prevenire il contagio comportano, in alcuni ambiti, la conoscibilità da parte del datore di lavoro di dati attinenti le condizioni di salute dei dipendenti. Ciò rappresenta una deroga ai principi ordinari attinenti la disciplina della protezione dei dati nei rapporti di lavoro.
L'intento dell'articolo è quello di analizzare gli equilibri delicati del rispetto dei diritti dei lavoratori nell'ambito dell'emergenza emersa a causa del COVID19.

Pandemic, emergency and data protection in the workplace:towards the resumption of productive activity

The picture that emerged from the pandemic situation in Europe leads to reflections that on the one hand touch on the particular profile of the data in circulation, the need for economic recovery.
One of the sectors inevitably involved in post-pandemic management is the management of workers' data in order to implement the preventive measures against compulsory accounting in all companies and organisations implementing the Prime Ministerial Decree of 11 March 2020. The same has provided for measures aimed at fostering the recovery of economic activity through the restoration of production activity limited to compliance with anti-accounting rules.
Compliance with the rules prepared in order to prevent contagion involves, in some areas, the availability to the employer of data concerning the health conditions of employees. This represents an exception to the ordinary principles of data protection in the workplace.
The intention of the article is to analyze the delicate balance of the respect of workers' rights in the context of the emergency arising from the COVID19.

Legal Tech e Informatica Giuridica

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 185-204

Dai *Dark Patterns* al *Legal Design*: problemi e soluzioni all'utilizzo degli elementi grafici per alterare la volontà degli utenti

Gabriele Ientile*

Indice: 1. Introduzione. – 2. Cosa sono i *Dark Patterns*. – 3. Dai *patterns* ai *Dark Patterns* passando per il *nudging*: storia ed evoluzione degli schemi nell'era digitale. – 4. Il *nudging* e la manipolazione del comportamento del consumatore – 5. Tipi, funzionamento e diffusione dei *Dark Patterns*. – 6. Normativa e giurisprudenza in tema di *Dark Patterns* e *nudging* – 7. L'opportunità del *Legal Desing* come soluzione al problema dei *Dark Patterns* – 8. Il *Legal Desing*: definizione e funzionamento – 9. Esempi di applicazione del *Legal Desing* ai *Dark Patterns* – 10. Conclusioni

1. *Introduzione*

L'avvento della riforma introdotta dal GDPR ha portato notevoli miglioramenti alla sicurezza dei dati degli utenti durante la navigazione, portando alla creazione di informative più dettagliate e spingendo molte aziende, digitali e non, a rendersi *compliant* con il Regolamento.

Nonostante ciò, le esperienze utente rimangono minacciate da numerose tecniche di persuasione inconscia, che tentano di sfruttare le zone grigie che esistono all'interno della normativa. Tra le tante si distinguono i *Dark Patterns*, che intaccano l'interfaccia grafica e sfruttano meccanismi inconsci al fine di far accettare informative che non sono state veramente lette, permettere la comunicazione dei propri dati a soggetti di cui si ignora la partecipazione al trattamento, acquistare prodotti che non si desiderano.

Scopo di questo articolo sarà, nella prima parte, analizzare i *Dark Patterns*: cosa sono, come si differenziano e come funzionano; successi-

* Praticante avvocato presso lo Studio Legale L&E, esperto di Privacy e Diritto di Internet. Practing Lawyer at L&E Law Firm, Privacy and Internet Law expert.

vamente si procederà a studiare il *Legal Desing* e spiegare perché rappresenta lo strumento migliore per colmare la zona grigia in cui vivono questi strumenti.

2. *Cosa sono i* Dark Patterns

Con il termine *Dark Patterns* ci si riferisce a quelle specifiche scelte stilistiche che permettono ad un servizio online di alterare il comportamento dell'utente in modo da far sì che «quest'ultimo prenda una decisione che non avrebbe preso nel caso in cui fosse stato informato o gli fosse stata concessa un'alternativa»[1]. In altri termini si tratta di modelli che impattano la struttura di una pagina web o di un applicativo mobile prevalentemente sotto il profilo grafico al fine di indurre l'utente a compiere scelte non consapevoli.

I *Dark Patterns* vengono utilizzati, pertanto, per trarre in confusione un utente e fargli accettare un servizio o una proposta contrattuale con termini differenti rispetto a quelli che si era figurato oppure privandolo della possibilità di negoziare. L'impiego di questi strumenti è concentrato, principalmente, su due fronti: (i) l'informativa privacy e il relativo consenso; (ii) l'e-commerce. La concentrazione in questi due ambiti è dovuta alla facilità con cui il prestatore del servizio ha un vantaggio immediato per il proprio business. Nel primo caso avrà facilmente accesso alle informazioni dell'utente e ai sensori del suo dispositivo, mentre nel secondo caso potrà facilmente indurre l'acquirente a comprare prodotti ulteriori rispetto a quelli inizialmente desiderati.

Ad oggi i *Dark Patterns* non sono stati oggetto di uno studio approfondito dal punto di vista legislativo ma sono stati analizzati, principalmente, da un punto di vista tecnico (per quanto concerne gli aspetti tecnici della strutturazione grafica di un sito web e la loro classificazione) e dal punto di vista etico (relativamente alle implicazioni etiche di costringere gli utenti a scelte forzate in uno spazio libero come il web).

[1] Cfr. A. Mathur, "*Dark Patterns* at Scale: Findings from a Crawl of 11K Shopping Websites", *Proc. ACM Hum. Comput. Interact.* Vol. 3, n. CSCW, Article 8, 2019.

Dai Dark Patterns *al* Legal Design*: problemi e soluzioni all'utilizzo degli elementi grafici per alterare la volontà degli utenti*

Già prima dell'introduzione del GDPR erano state sollevate numerose perplessità sulle modalità di raccolta del consenso degli interessati al trattamento. In questo contesto, l'accettazione delle cookie policy e delle privacy policy ha da sempre rappresentato motivo di discussione, in ragione del fatto che sono di difficile comprensione e difficilmente vengono approfondite dagli utenti.
Questo avviene per molteplici ragioni, tra cui l'utilizzo interfacce grafiche malevole, note come *Dark Patterns* della cui natura e funzionamento si discuterà nell'articolo. Lo scopo di questi strumenti è spingere gli utenti a prestare il proprio consenso senza soffermarsi sulle condizioni.
Al momento fenomeni di questo tipo vivono in una zona grigia dell'ordinamento, all'interno della quale non sono esplicitamente vietati, ma al tempo stesso contrastano con alcuni principi cardine della normativa in tema di protezione dei dati personali, tra cui la privacy by design.
I potenziali approcci al problema potrebbero operare sia ex ante che ex post. Introducendo un meccanismo sanzionatorio o dettando nuovi standard per la raccolta del consenso.
Una possibile soluzione potrebbe essere rappresentata dall'utilizzo del *Legal Design*, ossia l'introduzione di un approccio di *design-thinking* alla presentazione delle informazioni giuridiche.

From Dark Patterns to Legal Design: problems and remedies to the use of the graphic elements to alter user behavior

Even before the introduction of GDPR, a considerable number of doubts concerning the collection of the consent of the interested subjects was raised. In this context, the consent to privacy policy and cookie policy has always represented a discussed topic, due to its complexity. Moreover, users hardly focus on them.
This happens for several reasons, such as using malicious graphics, known as dark patterns, whose nature and function is discussed in this paper. The goal of this tools is to force user to accept the terms without focusing on them.
Currently this kind of phenomena stay in a "gray zone" of the law, inside which they are not expressly forbidden, but at the same time they are in opposition with some privacy law principles concerning personal data protection, such as privacy by design.
Potential approaches to this issue could work both ex ante and ex post, introducing new and specific fines and setting new standard regarding consent collection.
A potential solution could be represented by Legal Design, which is the introduction of a design-thinking method when displaying legal information.

Legal Tech e Informatica Giuridica

Ciberspazio e diritto, vol. 21, n. 64 (1 - 2020), pp. 207-224

Il fenomeno "pro-ana": alcune considerazioni informatico-giuridiche sui metodi di prevenzione e di contrasto

Andrea Scirpa*

Indice: 1. L'idea "pro-ana" come "stile di vita". – 2. Le fattispecie di reato. – 3. I metodi di prevenzione e contrasto al fenomeno "pro-ana": un approccio multidisciplinare.

La filosofia degli Ana:

1) *Non essere magri vuol dire non essere attraenti.*
2) *Essere magri è molto più importante che essere sani.*
3) *Devi comprare vestiti, tagliarti i capelli, assumere lassativi, morire di fame, fare qualsiasi cosa per farti sembrare più magro.*
4) *Non devi mangiare senza sentirti in colpa.*
5) *Non devi mangiare cibo ingrassante senza autopunirti dopo.*
6) *Devi contare le calorie e quindi restringerne l'assunzione.*
7) *Quello che dice la bilancia è la cosa più importante.*
8) *Perdere peso è bene / prendere peso è male.*
9) *Non puoi mai essere troppo magro.*
10) *Essere magro e non mangiare sono simbolo di vera forza di volontà e successo*.

(www.myhelpforum.net)

1. *L'idea "pro-ana" come "stile di vita"*

Il tema dei disturbi del comportamento alimentare illustrati e "glorificati" sul web, significativamente descritto nel "manifesto" poco sopra riportato e ripreso da un sito web pro-anoressia, è stato sollevato per la prima volta negli Stati Uniti d'America attorno agli anni 1998/1999 e si è diffuso, poi, in maniera capillare anche in Europa e in Italia a partire dagli

* Assegnista di ricerca presso l'Università degli Studi di Milano, Research Fellow del Centro di Ricerca in "Information Society Law" dell'Università degli Studi di Milano, collabora con la Cattedra di "Informatica Giuridica" come cultore della materia ed è componente del Comitato di Redazione della Rivista Scientifica "Ciberspazio e Diritto". Avvocato e Direttore dell'Ufficio "Organizzazione e gestione della privacy" della Provincia autonoma di Trento.

anni 2002/2003[1] (http://www.psicoterapeutiinformazione.it/la-filosofia-ana-il-culto-dei-disturbi-del-comportamento-alimentare-su-internet/3/).

Quando l'interprete si riferisce al fenomeno "pro-ana" online ha in mente l'analisi di siti web nei quali giovani ragazze e/o ragazzi si uniscono, creano una comunità finalizzata alla condivisione di obiettivi di dimagrimento e si scambiano consigli su come evitare di mangiare e su come dimagrire. Il fine è quello di raggiungere un'ideale "perfezione" che, per i soggetti affetti da anoressia, equivale a "sentire e vedere le proprie ossa".

Per poter accedere a tali *forum* e gruppi chiusi come partecipante attiva, esiste una sorta di "selezione" che prevede l'invio, da parte dell'aspirante anoressica, di fotografie reali. Tale richiesta deve essere corredata dalla promessa di rendere pubblici sul web i propri obiettivi di dimagrimento e il loro percorso, al fine di testare i limiti sino ai quali la candidata è disposta a spingersi e tenendo una sorta di diario che documenti l'evoluzione del proprio disturbo alimentare.

Per molti giovani, l'idea "pro-ana" rappresenta un vero e proprio stile di vita da condividere in chat private o blog ad accesso pubblico, allo scopo di sostenere altri utenti, ed essere a loro volta sostenuti, nel momento in cui s'intraprenda una battaglia condivisa verso la magrezza assoluta.

Il fenomeno dei siti web pro-anoressia ha interessato – e tuttora, sta interessando – i media americani in quanto esempio clamoroso della pervasività dei disturbi del comportamento alimentare nei giovani e negli adolescenti.

In particolare, prendendo ad esempio uno studio di Lyng[2] incentrato sul concetto di *edgework*, la sociologa Gailey ritiene, correttamente, che le comunità "pro-ana" siano un esempio di sottocultura (o sub-cultura che dir si voglia). Ciò pare derivare dal fatto che i suoi membri siano legati da simboli, immagini e da una sorta di linguaggio "segreto" in grado di generare uno stile di vita non sano, continuamente soggetto ad approvazione pubblica e, soprattutto, pericolosamente condiviso da tutti i partecipanti[3].

[1] E.D. Matteis, "La filosofia Ana: il culto dei disturbi del comportamento alimentare su internet", «Psicoterapia in – formazione», 4, 2009, pp. 74-93.

[2] S. Lyng, "Edgework: A social psichological analysis of voluntary risk-taking", «American Journal of Sociology», 95, 1990, pp. 851-856.

[3] J. Gailey, "Starving is the most fun a girl can have: The Pro-Ana Subculture as Edgework", «Critical criminology», 17(2), 2009, pp. 93-108.

Il fenomeno "pro-ana": alcune considerazioni informatico-giuridiche sui metodi di prevenzione e di contrasto

Lo sviluppo della società legato all'incremento dell'utilizzo delle nuove tecnologie è sicuramente indice di crescita sociale; come in qualunque ambito, però, se utilizzate in maniera errata e "fuori-controllo", producono effetti collaterali e, talvolta, nocivi per colui che ne abusa.
La crescita esponenziale dei siti web "pro-ana" ne è l'esempio: la malattia psichiatrica dell'anoressia, seppure tutt'oggi risulta un "tabù" o, in ogni caso, viene percepita come un "capriccio" delle adolescenti nella vita reale, nel cyberspazio assume un grado di pericolosità elevato.
Giovani donne che si scambiano sul web consigli su come dimagrire e mostrare finalmente le loro "splendide ossa", nella vita reale difficilmente parlano del loro disturbo alimentare con amici e parenti e, anzi, per la maggior parte, tendono a nascondere e rinnegare la malattia che le affligge.
Sebbene la legge dello Stato abbia tentato, e stia tutt'oggi tentando di contrastare e prevenire tale fenomeno, alla luce di quanto esposto nel presente studio, appare necessario un intervento multidisciplinare che preveda non solo una corretta punizione per coloro che istigano a disturbi del comportamento alimentare, ma anche un programma di prevenzione ed educazione di adolescenti, genitori ed insegnanti.
Riuscire a riconoscere un soggetto a rischio è già, di per sé, utile a prevenire l'aggravarsi della malattia e, dunque, l'uso/abuso di Internet come manuale di istruzione e fonte di ispirazione alla magrezza assoluta.

The "pro-ana" phenomenon: some IT-legal considerations on prevention and contrast methods

The development of society linked to the increased use of new technologies is certainly an indication of social growth; if used incorrectly, they can produce collateral effects
and sometimes it can be dangerous to the one who abuses it.
The diffusion of "pro-ana" web sites is an example: in real life, the psychiatric disease of anorexia nervosa is perceived as a "whim" of adolescents, while in cyberspace it takes an high degree of danger.
Very young women who exchange tips on how to lose weight on the web, in real life hardly talk about their eating disorder with friends and relatives.
Even if law tried, and is still trying, to fight and prevent this phenomenon, a multidisciplinary intervention is necessary.
Being able to recognize a person at risk is useful to prevent the disease and then the use and abuse of the web like an absolute thinness inspiration.