Le politiche digitali nella Repubblica Popolare Cinese

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 5-24

La disciplina dell'algoritmo nella Repubblica Popolare Cinese

Riccardo Berti*

Sommario: 1. Introduzione. – 2. La disciplina dell'algoritmo in Cina. – 3. L'intelligenza artificiale nel sistema giudiziario cinese. – 4. Conclusioni.

1. *Introduzione*

La Repubblica Popolare Cinese è estremamente attiva nel disciplinare il fenomeno informatico, che nel Paese è visto come un asset fondamentale da sviluppare, tutelare e (in certa misura) limitare. Il "cuore pulsante" della normativa cinese sul tema risiede nella "Cybersecurity Law of the People's Republic of China"[1], adottata nel 2016 e che, tra le varie prescrizioni, impone la residenza dei dati su suolo cinese in tutta una serie di infrastrutture critiche.

L'approccio cinese è, quindi, quello della tutela del "dato", a prescindere dalla sua natura di dato personale o meno, ed è proprio tenendo conto di questo approccio più ampio che si sono sviluppate anche le iniziative legislative più recenti, come la "Data Security Law"[2], una disciplina anch'essa dedicata alla governance ed alla tutela (e localizzazione sul territorio cinese) di tutti i dati informatici adottata nel 2021.

Parallelamente, anche a fronte delle preoccupazioni della popolazione cinese in relazione alla tutela dei dati personali e dell'allarme sociale destato dalla sempre più massiccia disponibilità di dati online, che ha

[1] 中华人民共和国网络安全法, adottata il 7 novembre 2016 ed in vigore dal primo giugno 2017.

[2] Data Security Law of the People's Republic of China (中华人民共和国数据安全法), adottata dal tredicesimo National People's Congress il 10 giugno 2021 e in vigore dal primo settembre dello stesso anno.

doi 10.53148/CD202401001

estremizzato il fenomeno della c.d. *human flesh search*[3], si è sviluppata una disciplina dedicata alla protezione dei dati personali, il cui più recente e organico sviluppo è la "Personal Information Protection Law of the People's Republic of China" (PIPL)[4], adottata anch'essa nel 2021.

Quest'ultima normativa contiene una prima fondamentale disciplina a tutela delle persone fisiche di fronte alle decisioni algoritmiche, molto simile a quella di cui all'art. 22 Regolamento UE 679/2016.

L'articolo 24 della PIPL cinese, infatti, dispone:

> Where personal information processors use personal information to make automatic decision, the transparency of decision-making and the fairness and justice of the results shall be ensured, and shall not impose unreasonable differential treatment on individuals in terms of transaction price and other transaction conditions. Where business marketing and information push are carried out through automatic decision-making, options not based on his/her personal characteristics shall be provided at the same time, or a convenient way for individuals to reject shall be provided. Where automatic decision-making has a significant impact on individual's rights and interests, he/she has the right to require the personal information processor to give an explanation, and to reject the decision made by the personal information processor only through automatic decision-making.

Il sistema cinese innesta, quindi, in uno schema molto simile a quello di cui alla normativa comunitaria, una disciplina specifica in relazione ai contenuti personalizzati, che devono consentire una forma di *opt-out* (che nella corrispondente disciplina comunitaria è, invece, previsto unicamente per i «fornitori di piattaforme online di dimensioni molto grandi» a mente del Digital Services Act) e permettere agli utenti di fruire di una esperienza non profilata.

[3] In cinese: *rénròu sōusuǒ* 人肉搜, ovvero lo sforzo collaborativo e massivo da parte di *netizens* cinesi che si impegnano a risolvere "casi" che balzano agli onori della cronaca, con effetti spesso distorti che portano a minacce e anche violenze nel mondo virtuale o fisico (cfr. Q. Bu, "'Human Flesh Search' in China: The Double-edged Sword", «International Data Privacy Law», vol. 3, n. 3, 2013, pp. 181-96).

[4] 中华人民共和国个人信息保护法, adottata dal tredicesimo National People's Congress il 10 giugno 2021 e in vigore dal primo settembre dello stesso anno, il cui testo inglese è disponibile sul sito del National People Congress al link http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (ultimo accesso in data 28.06.2023).

La disciplina dell'algoritmo nella Repubblica Popolare Cinese

L'evoluzione tecnologica rappresenta una sfida estremamente difficile da affrontare per i Legislatori, posti di fronte ad un fenomeno che evolve in tempi molto più veloci rispetto alla loro capacità regolatoria.
In questo contesto complesso, il modello occidentale, declinato nelle sue "varianti" europea e statunitense, è solitamente quello preso a riferimento nell'esaminare la disciplina dell'argomento. Non si tratta, però, dell'unico da prendere in considerazione quando si parla di normare le nuove tecnologie, specie nelle ultime problematiche declinazioni del fenomeno tecnologico/informatico, come quelle che derivano dalle più recenti innovazioni in tema di intelligenza artificiale.
Tra le produzioni normative non occidentali che si distinguono nel settore (come, ad esempio, quella indiana e giapponese) spesso trascurata è l'iniziativa della Repubblica Popolare Cinese, che pur è la culla di numerose nuove tecnologie e contende in altri casi il primato agli Stati Uniti.
Nel presente approfondimento si prenderanno in considerazione le più recenti normative sul tema della regolamentazione dell'algoritmo adottate nella Repubblica Popolare unitamente ad alcuni esempi di declinazione dell'intelligenza artificiale nella pratica giudiziaria, che dimostrano plasticamente la distanza fra un approccio normativo assimilabile a quello occidentale (e che, anzi, in certi punti presenta originali innovazioni) e un'applicazione pratica più distante dall'interpretazione dei principi in tema di tutela di utenti e dati personali cui si è abituati in occidente.

The discipline of the algorithm in the People's Republic of China

Technological evolution represents an extremely difficult challenge for Legislators, faced with a phenomenon that evolves much faster than their regulatory capacity.
In this complex context, the Western model, expressed in its European and American "variants", is usually the one taken as reference when examining the discipline of the topic. However, it is not the only one to take into consideration when talking about regulating new technologies, especially in the latest problematic declinations of the IT phenomenon such as those resulting from the most recent innovations in the field of artificial intelligence.
Among the non-Western regulatory productions that stand out in the sector (such as, for example, the Indian and Japanese ones), the initiative of the People's

Republic of China is often overlooked, although it is the cradle of numerous new technologies and in other cases competes for primacy with United States.
In this study, we will take into consideration the most recent regulations on the topic of algorithm regulation adopted in the People's Republic, together with some examples of the declination of artificial intelligence in judicial practice in the Country, which clearly demonstrate the distance from the regulatory approach of the West (approach that, in certain regards, presents original innovations) and a practical application that is far from the interpretation of the principles regarding the protection of users and personal data to which we are accustomed in the West.

L'era delle Smart Cities:
gestione dei dati e tutela dei cittadini

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 27-42

Smart cities: data governance e cooperative di dati al servizio delle c.d. "città intelligenti"

Virginia Putortì*, Tommaso Bratina**

Sommario: 1. Verso la realizzazione delle smart cities. – 1.1. Il concetto di smart city. – 1.2. La necessaria definizione di un piano di governance. – 2. Piattaforme co-op e sviluppo mutualistico dei servizi digitali per le smart cities. – 3. Conclusioni.

1. *Verso la realizzazione delle smart cities*

1.1. *Il concetto di smart city*

Una città "ideale", oggi, è quella in cui è possibile svolgere attività essenziali come raggiungere il posto di lavoro, andare a scuola o a fare la spesa, entro un massimo di 15 minuti a piedi dalla propria abitazione, riducendo la dipendenza dall'uso dei mezzi di trasporto e promuovendo gli spostamenti a piedi o in bicicletta. Questo modello di città è al centro della proposta di pianificazione urbana teorizzata dall'urbanista Carlos Moreno, la c.d. *15-minutes city*, una delle più recenti dimostrazioni di quanto le esigenze dei cittadini siano mutate negli ultimi anni.

Attraverso la nozione di "città intelligente" ci si riferisce alla gestione delle questioni legate alle realtà urbane attraverso un uso intelligente delle tecnologie dell'informazione e della comunicazione, ma non esiste, ad oggi, una definizione condivisa di cosa sia una città intelligente. Con l'evolversi del concetto di smart city, si è passati da un ideale fortemente orientato alla tecnologia ad un altro più incentrato sui cittadini, che mira ad affrontare la resilienza e lo sviluppo sostenibile delle città[1].

* Avvocata del Foro di Milano e Associate delle *practice areas* Data Protection & Cybersecurity e White-collar crime & Internal investigations dello Studio Legale Chiomenti (Milano).

** Junior Associate delle practice areas Data Protection & Cybersecurity e White-collar crime & Internal investigations" dello Studio Legale Chiomenti (Milano).

doi 10.53148/CD202401002

Per alcuni, una smart city, nel senso più ampio del termine, non è altro che un sistema di soluzioni tecnologiche che i governi e/o gli enti privati adottano al fine di migliorare la gestione e lo sviluppo delle città stesse. Tali soluzioni tecnologiche possono comprendere anche l'utilizzo di videocamere e sensori per raccogliere e analizzare dati per scopi quali, ad esempio, ridurre il traffico, potenziare la sicurezza di veicoli e pedoni[2], la sicurezza pubblica e i servizi di emergenza, fornire servizi di trasporto accessibili, migliorare la pianificazione e la progettazione civica, facilitare la ricerca e lo sviluppo[3].

Il concetto di smart city è stato introdotto per la prima volta nel 1990 con il fine di incorporare hardware e software avanzati basati sulle tecnologie dell'informazione e della comunicazione (ICT) all'interno della pianificazione urbana[4]. Molte cose sono cambiate da allora, dallo sviluppo delle nuove tecnologie alla reazione della società al loro incessante progredire e permeare la quotidianità dei cittadini, fino alla risposta – attiva o reattiva – delle istituzioni.

Qualunque sia il significato attribuito alle smart cities, tra le maggiori implicazioni vi sono quelle legate alla mole dei dati raccolti e a come trattarli. Nel presente scritto verranno analizzati alcuni profili critici – e attualmente molto discussi – legati al trattamento dei dati personali nel contesto

[1] Cfr. J. Franke, P. Gailhofer, *Data Governance and Regulation for Sustainable Smart Cities*, «Frontiers in Sustainable Cities», 2021, p. 1.

[2] Sul sopra citato tema della videosorveglianza, certamente ricompreso tra gli strumenti di cui una smart city potrebbe fruire, il Garante per la protezione dei dati personali (Garante Privacy) ha sanzionato un Comune per aver installato delle telecamere al fine di controllare chi trasgredisce alle regole sulla raccolta differenziata, limitandosi a fornire ai cittadini un'informativa c.d. "di primo livello", mediante cartello apposto su un cassonetto e privo di tutte le informazioni richieste dalla normativa. Nel caso di specie, il Garante Privacy ha rimarcato come il trattamento di dati personali mediante sistemi di videosorveglianza da parte di soggetti pubblici sia ammesso solo se necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (in questo caso, il Comune) o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso. Cfr. Provvedimento del Garante Privacy del 18 luglio 2023, n. 312, p. 5. Da ultimo, con riferimento al tema dell'intelligenza artificiale, si veda il Provvedimento del Garante Privacy dell'11 gennaio 2024, n. 9977020.

[3] Cfr. J. Johnson et al., *Data Governance Frameworks for Smart Cities: Key Considerations for Data Management and Use*, «J. L. & Mob.», vol. 1, 2022, p. 3.

[4] Cfr. R. Al Sharif, S. Pokharel, *Smart City Dimensions and Associated Risks: Review of literature,* «Sustainable Cities and Society», vol. 77, 2022, p.1.

Smart cities: data governance e cooperative di dati al servizio delle c.d. "città intelligenti"

Il presente elaborato si pone come obiettivo quello di fornire degli spunti di riflessione sul nuovo fenomeno delle c.d. "smart cities" partendo dalle più recenti iniziative avanzate in ambito europeo e soffermandosi su alcuni tra i profili più dibattuti, tra cui in particolare quello della data governance. In relazione a quest'ultimo aspetto, gli Autori si soffermano sull'istituto della cooperativa di dati che, collocato all'interno del framework della European Data Strategy, sembra porsi come utile strumento al servizio delle città intelligenti e, in tale contesto, come mezzo per rafforzare il controllo sui propri dati da parte dei cittadini.

Smart cities: data governance and data cooperatives at the service of smart cities

This Paper aims to provide insights on the new phenomenon of the so-called "smart cities", on the most recent initiatives brought forward in the European context as well as on some of the most discussed issues, including in particular that of data governance. In relation to the latter, the Authors dwell on the institution of the data cooperative, which, placed within the framework of the European Data Strategy, seems to serve as a useful tool for smart cities and, in this context, as a means for citizens to strengthen control over their own data.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 43-58

Intelligenza urbana: città intelligenti a prova di privacy

Susanna Viggiani*

Sommario: 1. Smart city: la nuova città intelligente. – 2. Coordinate normative. – 3. Smart city e pubblici poteri. – 4. Misure di sicurezza per una smart city a norma. – 5. Applicazioni pratiche di smart city: la *smart mobility*.

1. *Smart city: la nuova città intelligente*

Negli ultimi decenni il fenomeno dell'urbanizzazione, pur atteggiandosi con tratti differenti in considerazione del grado di sviluppo socio-economico delle varie realtà territoriali, ha consentito alle città di acquisire grande centralità nel processo di sviluppo economico, ambientale e sociale, anche alla luce dell'introduzione delle nuove tecnologie. In tale contesto, le città intelligenti costituiscono la nuova espressione dello sviluppo urbano. Invero, il neologismo "smart city"[1], pur non trovando una definizione all'interno dei testi legislativi, è ormai entrato a far parte del lessico comune delle organizzazioni politiche. Il termine smart, infatti, viene impiegato perché le città rappresentano il terreno di formazione delle politiche smart, fondate sull'utilizzo di mezzi tecnologici per la realizzazione di opere pubbliche di innovazione e inclusione sociale. Le smart cities rappresentano città contrassegnate dall'integrazione tra strutture e mezzi tecnologicamente avanzati, proiettate verso politiche di crescita sostenibile, create allo sco-

* Dott.ssa in giurisprudenza, Consulente Legale & Privacy Confartigianato Bologna Metropolitana, Specializzata in studi sull'amministrazione pubblica (SPISA).

[1] Cfr. P. Urbani, "La riforma del governo locale: dalle funzioni al governo degli interessi locali", intervento al convegno organizzato da Italia Decide, svoltosi a Roma, Camera dei deputati, il 30 novembre 2015, dal titolo "Ricostruire un equilibrio per il governo locale: comune, nuova area vasta, città metropolitana", il quale rileva che «storicamente l'esistenza delle amministrazioni locali si giustifica in primo luogo per soddisfare le esigenze di sviluppo economico e sociale delle comunità rappresentate, migliorare i[…] luoghi di vita e di lavoro, realizzare un assetto condiviso delle condizioni di sostenibilità dei propri territori […]».

po di conseguire un miglioramento degli standard qualitativi della vita di coloro che le abitano (si pensi a titolo puramente esemplificativo all'illuminazione pubblica, distribuzione dell'energia, mobilità, gestione dei rifiuti, monitoraggio ambientale, gestione delle infrastrutture, modelli di governance, servizi, sono solo alcuni esempi degli ambiti su cui si può agire per rendere una città più intelligente ed innovativa). Già il Decreto Legge 18 ottobre 2012, n. 179, recante "Ulteriori misure urgenti per la crescita del Paese", convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221, all'art. 20, c. 16, si riferisce all'inclusione sociale intelligente, intesa come «capacità, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di offrire informazioni nonché progettare ed erogare servizi fruibili senza discriminazioni dai soggetti appartenenti a categorie deboli o svantaggiate e funzionali alla partecipazione alle attività delle comunità intelligenti.» In tale scenario, la comunità rappresenta un nuovo modo di intendere la vita urbana, intesa come la manifestazione più moderna del concetto di «cittadinanza amministrativa[2]», che implica la configurazione di uno *status* relativo ad uno specifico territorio, il quale genera di conseguenza situazioni giuridiche soggettive attive e passive collegate all'essere persona residente[3].

Nell'intenzione del Legislatore, la città si prospetta il luogo per una strategia fondata sulla riqualificazione ambientale e sul miglioramento delle condizioni economiche e sociali, dal momento che è proprio nella città che tutti gli aspetti relativi alla mobilità, alla distribuzione dell'energia e all'utilizzo delle tecnologie dell'informazione e comunicazione dovrebbero essere dotati di una maggiore connessione. I diritti che ne scaturiscono sono contenuti nella Carta della cittadinanza digitale di cui

[2] Cfr. C.E. Gallo, "La pluralità delle cittadinanze e la cittadinanza amministrativa", «Diritto amministrativo», vol. 3, 2002, p. 481 ss., il quale rileva che «la cittadinanza non è più riferita soltanto alla titolarità di diritti di tipo politico, ma invece alla titolarità di una serie di posizioni che sono variamente riconducibili all'individuo per il fatto di essere abitante di una determinata realtà».

[3] Cfr. C.E. Gallo, "La pluralità delle cittadinanze e la cittadinanza amministrativa", op. cit., p. 481 ss., il quale avverte, peraltro, che il collegamento con il territorio «non significa, ovviamente, che al cittadino in quanto tale, o meglio, all'uomo in quanto tale, non siano riconosciuti diritti e doveri in tutto il territorio nazionale, indipendentemente dalla collettività nella quale opera o si trova; ciò significa invece che la localizzazione all'interno di una formazione sociale è il punto di riferimento normale del diritto, proprio in considerazione della socialità naturale e necessaria della persona umana».

L'intelligenza urbana: città intelligenti a prova di privacy

L'utilizzo di sistemi intelligenti nel campo delle smart cities porta alla costruzione di una dimensione nuova nel rapporto tra Amministrazione e cittadini. In tale contesto, le nuove tecnologie, tramite sistemi di controllo centralizzati e una pervasiva raccolta di informazioni in tempo reale, permettono di dare vita a una vera e propria città intelligente. Si innestano, in quest'ottica, le politiche di rigenerazione urbana incentrate sui temi di sicurezza e controllo del territorio e della mobilità c.d. *smart mobility*.

Urban intelligence: privacy-proof smart cities

The use of intelligent systems in the field of smart cities leads to the construction of a new dimension in the relationship between Administration and citizens. In this context, new technologies, through centralised control systems and a pervasive collection of information in real time, make it possible to create a true smart city. Therefore, urban regeneration policies based on the themes of security and control of the territory, and so-called smart mobility are inserted in this perspective.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 59-72

Controllo tecnologico e sorveglianza: dalla teoria ai primi tentativi di quartieri "smart" in Trentino

Carlotta Maria Capizzi*

1. *Introduzione*

Come noto, lo sviluppo di sistemi di intelligenza artificiale (da qui in avanti: "AI") ha influenzato, influenza e influenzerà, anche, il comparto legale. In particolare, l'AI incide nel sistema penalistico, sia nella sua accezione sostanziale che in quella processuale. Nel caso di quest'ultima, a sua volta, l'AI è in grado d'incidere sia nella fase delle investigazioni, digitali e non, che nella fase più prettamente processuale, quindi quella legata allo svolgimento del procedimento penale. Seppur l'influenza dei sistemi di AI nel diritto penale sia stata ampiamente analizzata, sia in riferimento ai sistemi di prevenzione e repressione del crimine[1] che di redazione delle sentenze[2], non ci si è, ancora, soffermati sufficientemente sull'effetto che i sistemi di sorveglianza cittadina, basati su tecnologie di AI, abbiano (o possano avere) in riferimento alla tutela dei diritti legati alla privacy dei cittadini. A conferma di quanto appena esposto, si evidenzia come, in Italia, siano stati attivati[3] sistemi di sorveglianza cittadina

* Abilitata alla professione forense presso la Corte di Appello di Trento, ICT Compliance Specialist per la Capogruppo di un importante Gruppo bancario Italiano.

[1] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Random House USA Inc., 2017.

[2] H. Fry, *Hello World: Being Human in the Age of Algorithm*, London, Transworld Publisher Ltd, 2019.

[3] Il progetto Marvel è stato bloccato a inizio novembre 2023, a seguito di una pronuncia del Garante per la Protezione dei Dati Personali che ha giudicato insufficienti i

a Trento e Rovereto, senza che la notizia abbia avuto alcun tipo di risonanza mediatica, nonostante sia idonea a sollevare numerosi quesiti relativi alla tutela dei dati raccolti attraverso i suddetti sistemi di sorveglianza.

In generale, ci si potrebbe (e dovrebbe) chiedere quale sia la ratio dietro alla predisposizione di sistemi simili (che si avrà modo di indagare, si veda infra *4. Le città di Trento e Rovereto: un case study*) e quali siano gli obiettivi che i comuni trentini si propongono di raggiungere attraverso una sorveglianza "speciale" (si anticipa, fin da ora, che l'obiettivo principale dovrebbe essere quello di prevenzione del crimine).

In particolare, invece, ci si potrebbe (e dovrebbe) chiedere come avvenga il trattamento dei dati raccolti, se siano raccolti anche dati biometrici[4] e se questi siano, in alcun modo, conservati e, in tal caso, come.

Pare necessario, anche, evidenziare come sistemi simili di sorveglianza "speciale" non siano nuovi nel panorama internazionale[5] ma siano, tendenzialmente, caratterizzati da alcune criticità relative, appunto, alla raccolta, al trattamento e all'utilizzo dei dati che, inevitabilmente, vengono raccolti attraverso i sistemi stessi[6].

Tutto ciò premesso, ci si appresta ad indagare i sistemi introdotti dalle città di Trento e Rovereto nel 2022, evidenziandone eventuali aspetti critici, anche in relazione a sistemi di sorveglianza simili adottati all'estero. A tal fine è necessaria, tuttavia, una breve premessa relativa all'utilizzo dei sistemi di AI nel diritto penale. Quest'ultima si rende rilevante in quanto lo scopo principale dei sistemi di sorveglianza d'interesse

sistemi utilizzati per mantenere l'anonimato dei dati raccolti (di cui si dirà infra). La notizia: https://www.ansa.it/trentino/notizie/2023/11/04/bloccati-progetti-sulluso-dellai-persicurezza-urbana-a-trento_5a06ca07-a655-4936-8bb2-9c2146f3ee47.html.

[4] Definiti dal GDPR al suo art. 4 come "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

[5] Si pensi, ad esempio, ai sistemi di sorveglianza adottati da Cina, Israele e Stati Uniti.

[6] Ci si riferisce, in particolare, ai diritti connessi alla privacy che potrebbero essere violati laddove i sistemi di sorveglianza non fossero basati su una normativa sufficientemente chiara e precisa in relazione alla conservazione e ai dati raccolti, si veda a proposito, cfr., UN Office of the High Commissioner for Human Rights "The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights", 2014.

Controllo tecnologico e sorveglianza: dalla teoria ai primi tentativi di quartieri "smart" in Trentino

Lo sviluppo dell'intelligenza artificiale ha provocato e, verosimilmente, provocherà, cambiamenti significativi nell'amministrazione della giustizia. In particolare, il progresso tecnologico ha permesso lo sviluppo di sistemi automatizzati di prevenzione del crimine (sia attraverso la previsione delle aree geografiche maggiormente esposte alla commissione di reati che il calcolo della probabilità di recidiva di singoli soggetti). A tale progresso si è accompagnato, anche, lo sviluppo di sistemi di c.d. sorveglianza digitale volti, anch'essi, alla prevenzione dei reati tramite la sorveglianza "intelligente" di specifici quartieri cittadini. In particolare, tali sistemi sarebbero in grado di comunicare con le forze dell'ordine eventuali situazioni di possibile pericolo, permettendo (in teoria) la prevenzione di crimini di vario genere. In Italia, un esperimento di sorveglianza digitale è stato proposto dalle città di Trento e Rovereto. Tuttavia, tale sistema di sorveglianza digitale ha provocato la reazione del Garante della privacy, il quale ha bloccato lo sviluppo dei progetti.

Technological control and surveillance: from theory to the first attempts at 'smart' neighbourhoods in Trentino

The development of artificial intelligence has caused significant changes in the administration of justice. In particular, technological progress has enabled the development of automated crime prevention systems (both through the prediction of the geographical areas most exposed to the commission of crimes and the calculation of the probability of recidivism of individual subjects). This progress has also been accompanied by the development of so-called digital surveillance systems, which are also aimed at crime prevention through the 'intelligent' surveillance of specific city districts. In particular, these systems would be able to communicate possible dangerous situations with the police, allowing (in theory) the prevention of crimes of various kinds. In Italy, an experiment in digital surveillance was proposed by the cities of Trento and Rovereto. However, this digital surveillance system provoked the reaction of the privacy Guarantor, who blocked the development of the projects.

Le implicazioni giuridiche del mondo virtuale

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 75-90

Il diritto del (e nel) metaverso: framework normativo e prospettive regolatorie

Gian Marco Bovenzi*

1. *Introduzione*

Letteralmente, può definirsi 'metaverso', termine apparso per la prima volta nel romanzo di Neal Stephenson "Snow Crash" del 1992, un concetto di spazio oltre (*meta*) l'universo[1]. Essendo ad oggi carente una precisa tassonomia delle sue caratteristiche strutturali e definitorie, è innanzitutto utile comprendere quali sono le tecnologie utilizzate nello sviluppo delle piattaforme.

Trattasi di tecnologie applicative di realtà virtuale (c.d. V.R., *virtual reality*) capaci di ricreare, attraverso una combinazione sinergica di software e hardware, un ambiente online tridimensionale immersivo, interattivo e capace di ivi simulare la presenza fisica di un utente[2]; e di tecnologie applicative di realtà aumentata (c.d. A.R., *augmented reality*), che consente all'u-

* Avvocato e dottorando di ricerca presso il Centro Alti Studi per la Difesa, ha conseguito un master di II Livello in Scienze Forensi, un LL.M. in American Law e un Certificate of Advanced Studies in National Security presso la l'Università di Syracuse (USA).

[1] Cfr. Accademia della Crusca, "Metaverso", 2022, disponibile al link https://accademiadellacrusca.it/it/parole-nuove/metaverso/21513#:~:text=Etimologia,universe%20'universo' (ultimo accesso in data 18 maggio 2023).

[2] Cfr. S. Bryson, "Virtual reality: A definition history-a personal essay", 2013, disponibile al link https://arXiv:1312.4322 (ultimo accesso in data 18 maggio 2023); Cfr. J. Steuer, "Defining Virtual Reality: Dimensions Determining Telepresence", «Journal of Communication», vol. 42, 1992, pp. 73-93.

tente di osservare, sempre attraverso l'ausilio di devices di supporto, il mondo reale con proiezioni virtuali sovrapposte agli stessi oggetti reali[3]: mentre la prima offre all'utente una percezione di immersività pressoché totale, nel secondo caso la percezione di immersività è ridotta e l'utente vive un'esperienza ibrida[4]. Le infrastrutture del metaverso possono poi essere costruite con tecnologie di M.R. (*mixed reality*), termine che indica convergenza tra A.R. e V.R. e descrive un continuum «between totally real and totally virtual environments»[5], e di X.R. (*extended reality*), termine onnicomprensivo di tutte le tecnologie immersive appena citate che forniscono agli utenti esperienze capaci di «blur the line»[6] tra il reale e il virtuale attraverso l'utilizzo di supporti visivi, auditivi, tattili e potenzialmente olfattivi.

Pertanto, può affermarsi con sufficiente precisione che il metaverso è definibile come una piattaforma digitale tridimensionale e relativamente immersiva sviluppata attraverso l'utilizzo combinato, e non necessariamente contestuale, di IoT, A.R., V.R., M.R. e componenti di intelligenza artificiale, in cui la realtà aumentata vissuta dall'utente è in grado di far percepire allo stesso delle esperienze simili alla vita reale. L'identità dell'utente nel metaverso è poi rappresentata dall'avatar in un ambiente misto tra cyberspazio e dimensione fisica[7], e con caratteristiche di ubiquità, interoperabilità e scalabilità[8], nonché persistenza, economicità e identità[9].

[3] Cfr. R.T. Azuma, "A Survey of Augmented Reality", «Presence: Teleoperators and Virtual Environments (MIT press)», vol. 6, n. 4, 1997, pp. 355-385.

[4] Cfr. C. Isola, "Augmented Reality, Advertising and consumer protection in the light of European Union Law", «Actualidad Jurídica Iberoamericana», vol. 18, febbraio 2023, pp. 1478-1509.

[5] Cfr. P. Milgram, F. Kishino, "A taxonomy of mixed reality visual displays", «IEICE Transactions on Information and Systems», vol. 77, n. 12, 1994, 1321-1329.

[6] Cfr. S. Alizadehsalehi, A. Hadavi, J.C. Huang, "From BIM to extended reality in AEC industry", «Automation in Construction», vol. 116, 2020.

[7] Cfr. S. Kasiyanto, M.R. Kilinc, "The Legal Conundrums of the Metaverse", «Journal of Central Banking Law and Institutions», vol. 1, n. 2, 2022, pp. 299-322.

[8] Cfr. European Parliament, "Metaverse. Opportunities, risks and policy implications", 2022, disponibile al link https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557 (ultimo accesso in data 21 maggio 2023). Cfr. J.D.N. Dioniso, W.G. Burns III, R. Gilbert, "3D Virtual worlds and the metaverse: Current status and future possibilities", «ACM Computing Surveys», vol. 45, n. 3, articolo n. 34, 2013, pp 1-38.

[9] Cfr. M. Ball, "The Metaverse: What It Is, Where to Find it, and Who Will Build It", 2020, disponibile al link https://www.matthewball.vc/all/themetaverse (ultimo

Il diritto del (e nel) metaverso: framework normativo e prospettive regolatorie

Il presente Contributo offre una breve sistematizzazione delle fonti del diritto dell'Unione Europea applicabili al metaverso. Dopo un'introduzione in cui si evidenziano le caratteristiche tecnico-definitorie del metaverso, il secondo paragrafo si sofferma sulle sue potenziali applicazioni e le possibili attività ivi espletabili. Il terzo paragrafo evidenzia le principali problematiche di natura giuridica che l'utilizzo non (o scarsamente) regolamentato dei mondi virtuali può sollevare in diversi settori del diritto. Dopo una disamina delle nuove iniziative da parte della Commissione europea ancora in attesa di definizione e/o entrata in vigore, si conclude affermando che il framework delle norme applicabili, pur se (ancora) adeguato allo stato tecnologico attuale, impone una urgente rivisitazione in chiave prospettica e dei futuri sviluppi del metaverso.

The law of (and in) the metaverse: legal framework and prospective regulations

The present contribution offers a brief systematization of the EU regulatory framework applicable to the metaverse. The introduction highlights technical features of the metaverse, while the second paragraph explores its potential applications and the activities that may be carried out by its users. The third paragraph assesses the main legal conundrums in several legal fields that might arise from a non-regulated (or improperly regulated) use of this virtual environment. After an overview of the new – yet pending – initiatives of the european Commission in the sector, the article concludes stating that although the legal framework appears adequate at the state of the current technological development, in light of the future developments of the metaverse more efforts are required in order to prevent its misuses.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 91-112

Declinazioni "phygital" di fenomeni devianti e criminali e loro lettura giuridica

Michelangelo Pascali*

Sommario: 1. Percezioni, rappresentazioni ed essenze del metaverso. – 2. Fenomenologia delle dinamiche sociali tra espressività digitale e sostanza reale. – 3. Le dimensionalità dell'agire violento. – 4. Novità tecno-sociali e tenuta del diritto.

1. *Percezioni, rappresentazioni ed essenze del metaverso*

La comparsa del metaverso, inteso come ambiente universale capace di costituire e intercettare la complessità della rete delle connessioni sociali in una nuova tipica estensione digitale, appare un evento, per quanto dai tratti non omogenei e lineari, dagli esiti potenzialmente dirompenti riguardo alla lettura della realtà secondo canoni consolidati.

In particolare, l'innovazione prodotta non può essere ridotta a un processo di mera trasposizione di una realtà concreta – in quanto "extra-informatica" – mediante un'"internetizzazione" di ultima generazione, ma va assunta come tassello di un *iter* costitutivo di un proprio reale, che vede precisamente la proprietà della sua essenza nella non separazione tra le sfere dell'esistenza.

Se con il termine che lo definisce si può intendere quello spazio informatico tridimensionale all'interno del quale le persone fisiche sono in grado di operare, produrre e interagire in vario modo e con diverse finalità, attraverso strumenti e servizi sempre più personalizzati, l'universo digitale così costituito – dotato di persistenza e interattività fra ambiti interconnessi che consentono azioni e relazioni in tempo reale[1] – genera realtà non (più) fittizia, ma semmai implementata. Questa realtà affermata tecnologicamente, fatta di galassie o sobborghi informativi, non è dunque una dimensione

* Professore associato di Sociologia giuridica, della devianza e mutamento sociale presso il Dipartimento di Scienze sociali dell'Università degli Studi di Napoli "Federico II".

[1] M. Ball, *The Metaverse. And How It Will Revolutionize Everything*, New York, Liveright Publishing Corporation, 2022.

conclusamente altra o puramente parallela, bensì è un qualcosa di integrato o, meglio, è pensabile come parte di realtà reciprocamente integrate.

Posto che il suo sorgere è certo legato alla diffusione di risorse specifiche, alla base della sua ascesa si scorge un'accelerazione nelle applicazioni scientifiche, l'avanzamento dell'ecologia digitale e, per l'appunto, un'integrazione tecnologica virtuale-fisica[2]. Sebbene il termine attribuitogli possa essere utilizzato come etichetta in maniera non sempre concorde, veicolando accezioni pure divergenti, pare comunque che l'approdo a un piano *phygital* [3], ossia, assieme e inscindibilmente, fisico *e* digitale, attraverso quel percorso d'iperconnessione che ha già ampiamente ibridato le frontiere di una vita *onlife*[4], possa definirsi come un elemento comune di fondo.

Quantunque non sia ancora ben definito se ciò apporterà un qualche contributo a quell'auspicato maggior "antropocentrismo tecnologico" [5], e a prescindere dalla generale problematicità della figura del *prosumer* sul piano informatico-reale dei diritti economico-commerciali, in equilibrio instabile tra libertà e imposizione[6], va poi marcato il dato per cui l'utente del mondo generato da questa maturazione scientifica tende a farsi sia consumatore sia produttore di idee, sino quasi a essere un propulsore d'innovazione, generando così un'inevitabile, ancorché non totale, orizzontalità di contenuti, con tutto quel che ciò comporta.

Atteso che il metaverso appare, quindi, essere un concetto composito e un ambito complesso, sotto un profilo ontologico e da un punto di vista

[2] CICIR - China Institutes of Contemporary International Relations, "Metaverse and National Security Report 2021", 2021, disponibile al link https://mp.weixin.qq.com/s/hlN7k-_4ZSftpyE2qNAGeA.

[3] C.EU - Council of the European Union, General Secretariat, "Metaverse - Virtual world, real challenges", 2022, disponibile al link https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf.

[4] L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham-Heidelberg-NewYork-Dordrecht-London, Springer, 2015.

[5] M. Dertouzos, *The Unfinished Revolution. Human-Centered Computers and What They Can Do For Us*, New York, Harper Collins, 2001.

[6] M. Pascali, "The "activity of choice" on the Web and the production of intellectual property rights: the media consumption between free service and unpaid work", «Труды по Интеллектуальной Собственности / Works on Intellectual Property», vol. 40, n. 1, 2002, pp. 70-72.

Declinazioni "phygital" di fenomeni devianti e criminali e loro lettura giuridica

L'Articolo, andando a evidenziare le caratteristiche peculiari del metaverso, per le quali va problematizzata la classica dicotomia virtuale/reale, invita a riflettere sulle modalità di interpretazione teorica di talune manifestazioni devianti e illegali, nonché sulle pratiche di costituzione di inerenti modelli di contrasto. Mediante l'esame di alcuni aspetti delinquenziali *phygital* (ossia, assieme, fisici e digitali), è vagliata la tenuta di tradizionali schemi repressivi penali, rapportandone presupposti e caratteri con le specificità delle nuove e diverse realtà sprigionate dal mutamento socio-tecnologico analizzato. Sembrerebbe emergere, dunque, da tutto questo, la necessità di prospettare strumenti rielaborativi di classificazione di tali fenomeni sociali complessi e, conseguentemente, di implementare pertinenti forme operative di comprensione giuridica.

"Phygital" declinations of deviant and criminal phenomena and their legal interpretation

The article explores the unique characteristics of the metaverse, challenging the traditional dichotomy between virtual and real, and encouraging the reader to reflect on the theoretical frameworks used to interpret deviant and illegal behaviours as well as to develop effective strategies to tackle them. Upon analysing various aspects of "phygital" delinquency (i.e. physical-digital), this study examines the effectiveness of conventional criminal justice systems considering the peculiar specificities of the socio-technological changes that have emerged. From this analysis, therefore, arises the need to search for tools to revise the classification of such intricate social phenomena and, as a result, to introduce appropriate operational forms of legal comprehension.

L'innovazione tecnologica e la digital forensics

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 115-130

FIT (*Freezing Internet Tool*) per innovare la digital forensics: riflessioni sulla prova digitale *cross-border*

Ivana Genestrone[*], Giulia Tirozzi[**]

1. *Premessa*

La recente presentazione al pubblico di FIT (Freezing Internet Tool)[1], un software *open source* (più precisamente FLOSS[2]), pensato e sviluppato da informatici forensi per acquisire contenuti web, costituisce l'occasione per riflettere sulla natura particolare della prova digitale.

Ci si riferisce, in particolare, all'ipotesi in cui il "fatto" da dimostrare in giudizio consista in un "contenuto web" (da intendersi come qualsiasi

* L'avv. Ivana Genestrone del Foro di Lucca ha maturato una profonda esperienza nel settore della privacy e del diritto delle nuove tecnologie. Lead Auditor ISO 27001 e DPO in diverse realtà aziendali, ha integrato il suo Studio legale con la digital forensics.

** L'avv. Giulia Tirozzi del Foro di Lucca, è DPO, segue tematiche relative al diritto delle nuove tecnologie, si occupa di ISO 27001 e di digital forensics.

[1] Il software è stato presentato, per la prima volta, all'edizione di HackinBo del 10 giugno 2023 da parte del Dott. Fabio Zito (@zitelog) e della Dott.ssa Francesca Policelli (il video è disponibile al seguente link https://www.youtube.com/watch?v=h0r1sv40w6g, ultima consultazione del sito in data 30/12/2023). La descrizione di FIT riportata in questo Articolo si basa in larga parte su questa presentazione; il software è stato, successivamente, presentato, nel mese di ottobre 2023, al SANS di Praga dal Dott. Giovanni Bassetti (@nannib) e dal Dott. Domenico Palmisano, al Linux Day di Bari dal Prof. Ugo Lopez, e al Convegno ONIF ("Osservatorio Nazionale di Informatica Forense", https://www.onif.it/) dal Dott. Andrea Lazzarotto.

[2] Acronimo di Free/Libre/Open Source Software.

elemento che possa essere incluso all'interno di un documento HTML[3]), come può avvenire, per esempio, in un caso di diffamazione tramite blog o di cyberbullismo.

Una pagina web è composta, per sua natura, da contenuti particolarmente dinamici e volatili. Si pensi a post pubblicati su canali social, e gli eventuali commenti, che possono essere modificati velocemente e in maniera pesante, fino all'eliminazione di un contenuto che fino a poco tempo prima era pubblicato: in questo caso, affinché la prova resista in giudizio, non ci si può limitare alla produzione di uno screenshot della schermata che interessa, perché è, invece, necessario anche assicurare che la prova fornita al giudice sia autentica (riferibile al soggetto al quale si addebita l'azione in questione), integra (non manipolata) e non ripudiabile dal soggetto contro il quale la prova viene prodotta.

In molti casi, poi, occorre che la prova resista ad un "trattamento" *cross-border*, in quanto, per loro natura, gli elementi contenuti in una pagina web, trascendono in confini internazionali.

Nell'assenza di una definizione del Legislatore, sta emergendo una disciplina speciale della prova digitale quale risultato degli sforzi provenienti dalle varie "anime" professionali riguardate dalle indagini processuali: giurisprudenza[4], Forze dell'Ordine[5], dottrina[6], informatica forense[7].

[3] Cfr. Definizione suggerita dal Dott. Fabio Zito, presentazione di FIT Project a HackinBo, sopra citata.

[4] Tra le tante: Trib. Milano 6 giugno 2018, n. 6355 sull'ammissibilità della pagina web riprodotta tramite la *Wayback Machine* (archivio digitale del world wide web curato da Internet Archive, organizzazione no profit con sede a San Francisco, USA).

[5] Ci si riferisce qui alla Circolare n. 1/2018 della Guardia di Finanza, "Manuale operativo in materia di contrasto alle frodi e all'evasione fiscale": detta circolare, come si evince dal titolo, definisce direttive operative per le azioni di contrasto della Guardia di Finanza all'evasione e alle frodi fiscali ed economico finanziarie e, che, in particolare, per chi scrive, descrive le procedure, gli strumenti e le metodologie più adatti per le attività di acquisizione delle evidenze digitali.

[6] Cfr. L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, 2007; V. Colarocco, T. Grotto, G. Vaciago, *La prova digitale*, Milano, Giuffrè Francis Lefebvre, 2020; A. Larussa, P. Pellegrinelli, *Le prove digitali nel processo*, Milano, Utet Giuridica, 2023.

[7] Diverse sono le occasioni di confronto organizzate tra gli informatici forensi; con specifico riferimento a FIT ed alle riflessioni specialistiche che andrebbero considerate dal mondo legale, si richiama il sopra citato HackinBo e, in particolare, la presentazione del

*FIT (*Freezing Internet Tool*) per innovare la digital forensics: riflessioni sulla prova digitale cross-border*

Recentemente, è stato presentato al pubblico FIT (*Freezing Internet Tool*), un software open source, pensato e sviluppato da e per informatici forensi, con la finalità di acquisire evidenza documentale, utilizzabile in giudizio, di contenuti web dinamici (pagine social con commenti). L'evento offre l'occasione per riflettere sulla natura particolare della prova digitale e sulle norme che la governano, caratterizzate dalla multidisciplinarietà. Devono, infatti, essere rispettati requisiti tecnico-informatici per la raccolta, conservazione e trasmissione della prova digitale, in modo da assicurarne l'autenticità e l'integrità. Queste regole possono essere ravvisate nello standard ISO/IEC 27037:2012, riconoscibile in contesti *cross-border*. Contribuiscono a formare questa singolare disciplina le regole tecniche per la conservazione di contenuti web dinamici sviluppati dalle scienze archivistiche. Le riflessioni su FIT si chiudono motivando la meritevolezza di tutela da parte dell'ordinamento giuridico dell'applicazione, quando usata a fini di difesa.

FIT (Freezing Internet Tool) to innovate digital forensics: reflections on cross-border digital evidence

Recently, an open-source software called FIT (Freezing Internet Tool) was presented to the public. FIT has been developed by forensic computer experts to collect website and social media evidence, that may be relied on in court. The launch of this software gives us an opportunity to reflect on the unique nature of digital evidence and its rules, characterized by a multidisciplinary approach. In facts, technical and informatics requirements must be met for the collection, storage, and transmission of digital evidence to ensure its authenticity and integrity. These rules may be found in the standard ISO/IEC 27037:2012, which may be acknowledged in cross border investigations. Archival sciences have also contributed to the development of technical rules for preserving dynamic web evidence. The article concludes by highlighting the importance of the legal protection for the use of FIT when used for defence purposes.

Sicurezza cibernetica e protezione delle infrastrutture nell'Unione europea

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 133-150

Network and Information Security: la strategia europea nella Direttiva NIS II e le sfide che ci attendono

Claudia Ogriseg*

Sommario: 1. La strategia europea in tema di sicurezza informatica e il nuovo cyber framework europeo. – 2. Dalla direttiva NIS alla NIS II: l'impatto atteso con la revisione del campo di applicazione. – 3. Il sistema di cooperazione tra Stati sui temi della sicurezza informatica. – 4. La sicurezza informatica e la gestione multirischio. – 5. Gli obblighi di notifica e reportistica sugli incidenti. – 6. L'aggravamento delle sanzioni. – 7. Spunti conclusivi.

1. *La strategia europea in tema di sicurezza informatica e il nuovo cyber framework europeo*

I primi tasselli dell'ecosistema normativo di un mercato unico digitale europeo erano stati definiti con il Regolamento UE n. 2016/679 General Data Protection Regulation (GDPR) sulla protezione dei dati personali trattati nelle aziende e il Regolamento UE n. 2019/881 Cybersecurity Act in tema di certificazioni per i prodotti/servizi ad impatto tecnologico, da un lato, e la Direttiva UE n. 2016/1148 Network and Information Security (NIS) sulla sicurezza delle reti e dei sistemi informativi per Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD), dall'altro.

L'esigenza di novellare il descritto cyber framework e, più in particolare la Direttiva NIS, è emersa a seguito di un esame del quadro d'incertezza generale in cui versava il settore della sicurezza informatica, delineato in due valutazioni d'impatto della stessa Direttiva NIS[1]. La NIS impo-

* Dottore di ricerca in Diritto del Lavoro e Relazioni Industriali e Research Fellow dell'ISLC - Information Society Law Center svolge la professione forense e riveste il ruolo di Data Protection Officer per enti pubblici e strutture sanitarie.

[1] Così G. Marino, "Cybersecurity nell'UE: ecco le ragioni di una NIS2", «Agenda Digitale», 2022, disponibile al link https://www.agendadigitale.eu/sicurezza/cybersecurity-comune-nellue-ecco-le-ragioni-di-una-nis2/ (ultimo accesso in data 21 gennaio 2024).

neva agli Stati di introdurre obblighi di cybersicurezza ai soggetti che fornivano servizi o svolgevano attività economicamente rilevanti e ciò sul fondamento della base dell'art.114 TFUE per il rafforzamento del mercato interno[2]. Il recepimento della NIS è avvenuto con variazioni rilevanti in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza: "l'erosione" della sovranità digitale non era stata efficiente. Agli Stati membri è stata lasciata troppa discrezionalità nell'individuazione degli operatori economici essenziali (OSE), valutati come strategici per l'UE. L'espandersi della pandemia Covid-19 ha fatto emergere tutte le criticità della NIS derivanti dal fatto che le strutture ospedaliere non sempre erano destinatarie di specifiche misure e adempimenti per la sicurezza dei sistemi, risultando spesso escluse nel campo di applicazione.

Le analisi della Commissione europea sull'impatto della NIS hanno rilevato un basso livello di resilienza delle imprese dell'Unione europea; una sensibilità non omogenea nelle istituzioni dei Paesi membri; una mancanza di consapevolezza dell'importanza della disciplina oltre all'assenza di uno strumento capace di far fronte alla crisi. Inoltre, secondo le stime condotte, l'adozione di una policy di cybersecurity interessava solo il 27% delle piccole imprese, il 51% delle medie imprese, il 72% delle grandi imprese. Si delineava così, nell'ambito della Strategia dell'UE per la cybersicurezza del 2020[3], l'esigenza di un nuovo approccio alla cybersecurity coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche fondato sulla identificazione, valutazione e mitigazione del rischio informatico in settori strategici, sia a livello di governance sia a livello operativo, anche interessando la catena di approvvigionamento.

Risale alla fine del 2022 la pubblicazione di un pacchetto normativo volto a garantire una maggiore chiarezza giuridica e coerenza sui temi cyber contenente: il Regolamento UE n. 2022/2554 Digital Operational Resilience Act (DORA), la Direttiva UE n. 2022/2557 Critical Entities Resilience (CER), che sostituisce la direttiva europea sulle infrastrut-

[2] Cfr. S. Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, I Post di AISDUE, III (2021), Sezione "Atti convegni AISDUE", n. 5, 20 dicembre 2021 disponibile al link https://www.aisdue.eu/wp-content/uploads/2021/12/Poli-Bologna-1.pdf (ultimo accesso 21 gennaio 2024).

[3] Scaricabile al seguente link http://images.dirittounioneeuropea.eu/f/sentenze/documento_4Sd4I_D.

Network and Information Security: la strategia europea nella Direttiva NIS II e le sfide che ci attendono

L'Articolo analizza il trend dell'aggiornamento del cyber framework europeo alle previsioni contenute nella Direttiva Network Information Security II (cd. NIS II). Dall'esame delle nuove norme, che dovranno essere recepite negli Stati membri entro il prossimo ottobre 2024, ci si attende un impatto significativo per il mercato digitale europeo. Le disposizioni contenute nella Direttiva NIS II interesseranno non solo le realtà strategiche degli Stati membri e dello spazio europeo ma altresì le loro filiere imponendo un miglioramento dei profili di cyber sicurezza anche per le piccole e medie imprese. La strategia dell'Unione sviluppata nella Direttiva NIS II migliorerà la consapevolezza sulle misure da adottare e responsabilizzerà gli organi gestori delle "entità critiche". La valorizzazione dei sistemi di certificazione volontaria consentirà di disporre di uno strumento per l'organizzazione interna e la scelta dei fornitori. La responsabilizzazione degli organi gestori, li spingerà ad adottare consapevolmente un sistema di gestione multi-rischio e, a livello di governance, a scegliere e monitorare adeguatamente la propria supply chain con verifiche costanti e puntuali su ciascuna terza parte coinvolta. Non resta che attendere che normative nazionali e sistemi di certificazione promuovano l'adozione di concrete pratiche di sicurezza garantendo la protezione delle infrastrutture dei sistemi informatici e di rete, dell'hardware, del software e della sicurezza delle applicazioni online e dei dati aziendali o degli utenti finali.

Network and Information Security: the European strategy in the NIS II Directive and the challenges ahead

The Paper analyzes the trend of updating the European cyber framework to the provisions contained in the Network Information Security II Directive (so-called NIS II). From an examination of the new rules, which must be transposed in member states by next October 2024, a significant impact is expected for the European digital market. The provisions contained in the NIS II Directive will affect not only the strategic realities of the member states and the European space but also their supply chains by requiring improved cyber security profiles for small and medium-sized enterprises as well. The Union's strategy developed in the NIS II Directive will improve awareness of the measures to be taken and empower the managing bodies of "critical entities". The enhancement of voluntary certification systems will provide a tool for internal organization and supplier selection. Empowering the managing bodies, will prompt them to conscious-

ly adopt a multi-risk management system and, at the governance level, to properly choose and monitor their supply chain with constant and timely audits of each third party involved. Now all that remains is to wait for national regulations and certification systems to promote the adoption of concrete security practices by ensuring the protection of IT and network systems infrastructure, hardware, software, and the security of online applications and business or end-user data.

L'intelligenza artificiale e le sue applicazioni in diversi settori: tra riflessioni giuridiche ed etiche

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 153-176

Diritto e intelligenza artificiale generativa: l'istruttoria del Garante per la protezione dei dati italiano su OpenAI e ChatGPT

Gianluigi M. Riva*

1. *Introduzione*

Il 30 novembre del 2022, il servizio ChatGPT 3.0 (*Chat Generative Pre-Trained Transformer*) veniva lanciato a livello mondiale[1] dall'azienda americana OpenAI[2]. Questo chatbot, basato su tecnologia NLP (*Natural Language Processing* – elaborazione del linguaggio naturale), ha frantumato ogni precedente record raggiungendo i cento milioni di utenti in appena due mesi[3] e riportando in auge – c.d. *hype* – il dibattito sull'intel-

* Postdoctoral Research fellow presso l'Università Commerciale Luigi Bocconi dove si occupa di *Neuroprivacy* e *Human Enhancement* quale *P.I.* del progetto PRIME LIBERTIES. Fellow del Centro BAFFI – RULES e dell'Institute for European Policymaking presso Bocconi, Connection Science fellow presso il Massachusetts Institute of Technology, Media Lab (Fulbright-Shuman 2019/20), Research affiliate presso la University College Dublin, dove ha ottenuto un Ph.D. (Marie Curie) in *Privacy, Ethics and New Technology* e non-residential fellow presso l'Information Society Law Center dell'Università degli Studi di Milano.

[1] OpenAI, "ChatGPT: Optimizing Language Models for Dialogue", 2022, disponibile al link https://web.archive.org/web/20221130180912/https://openai.com/blog/chatgpt/(ultimo accesso 10.07.2023).

[2] OpenAI, "Creating safe AGI that benefits all of humanity", 2023, disponibile al link https://openai.com/ (ultimo accesso 10.07.2023).

[3] Cfr. M. Oliva, "ChatGPT: 100 milioni di utenti attivi in due mesi", disponibile al link https://www.punto-informatico.it/chatgpt-100-milioni-di-utenti-attivi-in-due-mesi/ (ultimo accesso 10.07.2023).

ligenza artificiale e sui suoi possibili sviluppi e rischi, financo in tema di reale "intelligenza" e coscienza delle macchine[4].

Lo scalpore destato dalla piattaforma di IA generativa ha orientato i riflettori tanto sulle capacità di questi modelli di LLM (*Large Language Models*), quanto, soprattutto, sulla mole di dati strutturati e non usati per l'addestramento dei modelli stessi e, fra questi, di dati personali. Tutti questi elementi hanno attirato l'attenzione dell'Autorità Garante per la Protezione dei Dati Personali, che ha aperto un'istruttoria e rapidamente emanato un provvedimento d'urgenza per la sospensione dei servizi di ChatGPT offerti in Italia da OpenAI[5]. Con tale atto, il Garante imponeva a OpenAI L.L.C. «la misura della limitazione provvisoria del trattamento» ai sensi dell'art. 58, par. 2, lett. f) del Regolamento Generale per la Protezione dei Dati dell'Unione europea (GDPR), disponendo nei confronti del titolare del trattamento *ut supra* un termine di venti giorni dalla data di ricezione del provvedimento per «comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto e di fornire ogni elemento ritenuto utile a giustificare le violazioni […] evidenziate».

Prendeva, così, il via l'*affaire* Garante vs. ChatGPT (*rectius:* vs. OpenAI), che, sin da subito, ha diviso sia i commentatori che i fruitori del servizio fra chi ha ritenuto sproporzionato e non necessario un intervento d'urgenza di tal guisa e chi, al contrario, ha valutato opportuno anteporre i principi del diritto, specie a protezione e tutela dei soggetti interessati – e più in generale della collettività – alle ragioni utilitaristiche dettate da un facile accesso ai servizi offerti a discapito di privacy e liceità del trattamento.

[4] Il dibattito sulla presunta coscienza delle *generative AI* è invero rimasto al di fuori – a oggi – da lavori strettamente scientifici, attestandosi più a livello mediatico e di approfondimenti divulgativi: cfr. K.L. Ong, S. Fatima, "ChatGPT – Sentient AI or singularity. How close are we?", 2.02.2023, disponibile al link https://www.rmit.edu.au/news/acumen/ChatGPT_sentientorsingularity (ultimo accesso 10.07.2023) e K. Collier, "What is consciousness? ChatGPT and advanced AI might redefine our answer", 28.02.2023, disponibile al link https://www.nbcnews.com/tech/tech-news/chatgpt-ai-consciousness-rcna71777 (ultimo accesso 10.07.2023), fra le molte fonti a livello internazionale. Non così, invece, per il precedente caso "LaMDA" che aveva effettivamente generato un confronto a livello accademico: cfr. M. Griffiths, "Is LaMDA sentient?", in «AI & Society», vol. 37, n. 4, ottobre 2022, disponibile al link https://doi.org/10.1007/s00146-022-01559-z (ultimo accesso 10.07.2023).

[5] Garante Privacy, "Provvedimento n. 112 del 30 marzo 2023 [doc-web n. 9870832]", disponibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 (ultimo accesso 10.07.2023).

Diritto e intelligenza artificiale generativa: l'istruttoria del Garante per la protezione dei dati italiano su OpenAI e ChatGPT

L'intelligenza artificiale (IA) generativa ha fatto irruzione nel mercato digitale grazie al lancio del servizio ChatGPT della società americana OpenAI, cui è seguito un *hype* di interesse e un nutrito dibattito sulle capacità e potenzialità di questi innovativi sistemi. L'attenzione destata da ChatGPT grazie al suo enorme e rapido successo globale ha allertato l'Autorità italiana Garante per la Protezione dei Dati Personali, che ha ritenuto di intervenire con un provvedimento d'urgenza per il blocco del servizio in Italia, salvo, poi, concedere la riabilitazione del servizio a talune specifiche condizioni. Questo articolo analizza il caso e i provvedimenti punto per punto, focalizzandosi sui temi presenti e quelli assenti nell'attività del Garante, nonché sull'efficacia delle misure adottate da OpenAI per la riattivazione del servizio. L'analisi del caso si iscrive in più ampie considerazioni socio-giuridiche sulla contrapposizione fra trattamento dati personali e progettazione di tecnologie innovative, ponendo l'accento sugli effetti che l'intervento del Garante potrebbe avere in altri contesti digitali. Dopo una breve introduzione al caso, l'articolo analizza i vari provvedimenti intervenuti e gli specifici contenuti degli stessi. In particolare, l'analisi si concentra sull'informativa, le basi giuridiche e le questioni di giurisdizione. Nelle conclusioni, il contributo rimarca le questioni etiche che possono derivare dal caso e valuta l'implementazione della *privacy by design* in chiave comparatistica UE-USA.

Law and generative Artificial Intelligence: the Italian Data Protection Authority's preliminary investigation on OpenAI and ChatGPT

Generative artificial intelligence (AI) has burst onto the digital market thanks to the launch of OpenAI's ChatGPT service, which was followed by a hype of interest and a lively debate on the capabilities and potentials of these innovative systems. The attention aroused by ChatGPT thanks to its enormous and rapid global success alerted the Italian Data Protection Authority (Garante), which decided to intervene with an emergency measure to block the service in Italy, but then granted the rehabilitation of the service under certain specific conditions. This article analyses the case and the measures, focusing on the present and absent elements in the action of the Garante, as well as on the effectiveness of the measures adopted by OpenAI to be able to reactivate the service. The analysis of the case is part of broader socio-legal considerations on the contrast between personal data processing and the design of innovative technologies and it highlights

the effects that the Garante's intervention could have in other digital contexts. After a brief introduction to the case, the article analyses the various measures and their contents. In particular, the analysis focuses on the information leaflet, legal bases, and jurisdiction issues. In the conclusions, the contribution stresses the ethical issues that may arise from the case and assesses the implementation of privacy by design from an EU-US comparative perspective.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 177-192

Lo statuto del robot fra personalità e responsabilità giuridica

Emanuele Brambilla*

Sommario: 1. Definizione di robot. – 2. Il robot è persona? – 3. Responsabilità umana e robotica.

1. *Definizione di robot*

Nei film di fantascienza, i robot sono esseri antropomorfi dotati di intelligenza e capacità di giudizio che, pur consapevoli di essere governati da complessi algoritmi, riescono in qualche modo ad affrancarsene, rivendicando un margine di libertà d'arbitrio[1].

Una rappresentazione del genere, a prescindere dagli scopi cinematografici, attribuisce qualità specificatamente umane ai robot, contribuendo a far passare l'idea che, talvolta, essi siano addirittura più umani di noi stessi, in quanto a responsabilità e retto giudizio.

Si provi ora a riflettere sul concetto di "robot", facendone emergere le principali caratteristiche, al fine di verificare se gli si possa attribuire lo statuto di persona e se possa essere considerato un agente pienamente responsabile.

In termini molto generali, il robot è una macchina artificiale programmabile, capace di svolgere determinate azioni che integrano o sostituiscono le capacità manuali e mentali dell'essere umano. Come sottolinea Laura Palazzani, in questa definizione rientrano tutte le differenze che sussistono fra i vari robot: non tutti, infatti, assomigliano all'uomo, sono dotati di intelligenza o hanno le stesse funzionalità. I robot che si muovo-

* Dottorando in Filosofia del diritto presso il Dipartimento di Scienze giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano e Research Fellow presso l'Information Society Law Center (ISLC).

[1] A ciò è connesso anche l'aspetto esterno di alcuni dispositivi che, presentando volti o sorrisi, divengono quasi antropomorfi. A. Fabris, *Etica per le tecnologie dell'informazione e della comunicazione*, Roma, Carocci, 2018, p. 73.

doi 10.53148/CD202401010

no solo sotto il controllo umano, per esempio, non avendo alcun margine di autonomia, non possono nemmeno essere considerati intelligenti[2].

A questo proposito, il Comitato Nazionale per la Bioetica e quello per la Biosicurezza, le Biotecnologie e le Scienze della Vita, nel documento intitolato *Sviluppi della robotica e della roboetica*, propongono una netta distinzione fra robot che posseggono un corpo artificiale e quelli che ne sono privi. A prima vista, parlare di robot senza un corpo sembra contraddirne sia la stessa definizione, che li descrive come macchine artificiali, sia il comune modo di rappresentarli. Tuttavia, ad un esame più attento dello scritto, il vero discrimine fra le due suddette tipologie, più che il possesso di un supporto artificiale, è la capacità di compiere determinati movimenti[3]. Così facendo, si associa indissolubilmente il supporto fisico alla capacità di relazione con ciò che lo circonda, tramite l'interattività delle sue parti meccaniche.

Un'ulteriore classificazione, riguardante entrambe le tipologie di robot, è il possesso o l'assenza di intelligenza, elemento fondamentale per poter parlare di personalità e responsabilità giuridica[4]. Gli studiosi, quando scrivono di robot "stupidi", si riferiscono a macchinari automatici per uso industriale o domestico capaci di movimento (dunque, provvisti di un supporto fisico) e a telefoni fissi, radio o televisori senza accesso a Internet, se sprovvisti di corpo. Come è evidente dagli esempi appena presentati, la mancanza di un movimento autonomo è il vero discrimi-

[2] Nel presente Contributo, ci si occuperà esclusivamente delle macchine più sofisticate e dotate di intelligenza artificiale, non avendo senso parlare di personalità o responsabilità robotica nel caso di dispositivi completamente guidati dall'uomo. L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale*, Roma, Studium, p. 41.

[3] «Avere un corpo significa essere in grado di attuare dei movimenti, cioè di produrre lavoro fisico, a differenza di un computer che non è in grado di fare alcun movimento cinematico-dinamico, cioè è immobile. I robot con il corpo possono essere "stupidi" o "intelligenti", cioè non dotati o dotati di capacità "cognitive" [virgolette nostre] e lo stesso vale per quelli senza corpo». È curioso notare come, nel caso di assenza del corpo, il robot equivalga di fatto al software (nel caso di robot intelligenti) o, per lo meno, ai circuiti interni di un dato dispositivo atti a generare input sonori o visivi. Comitato Nazionale per la Bioetica e Comitato Nazionale per la Bioetica e per la Biosicurezza, le Biotecnologie e le Scienze della Vita, *Sviluppi della robotica e della roboetica*, 17 luglio 2017, p. 7.

[4] Con "personalità" qui si intende il modo o la condizione di essere persona, senso in cui viene utilizzato il termine dall'Aquinate. Tommaso d'Aquino, *Summa Theologiae*, I, q. 39, a. 3.

Lo statuto del robot fra personalità e responsabilità giuridica

Al giorno d'oggi, i robot interagiscono costantemente con noi e sono utilizzati ovunque nelle nostre città, nei luoghi di lavoro e nelle case. L'articolo indaga la possibilità che un robot possa essere considerato una persona giuridica e analizza le responsabilità associate a tale riconoscimento.
La discussione prende in considerazione il panorama giuridico europeo e internazionale, seguendo due percorsi principali. In primo luogo, indaga sul concetto di persona giuridica, chiedendosi se sia appropriato attribuirlo a una macchina e come ciò possa essere compiuto. In secondo luogo, affronta il tema della responsabilità nel contesto delle azioni robotiche, esaminando le potenziali responsabilità dei dispositivi, degli utenti e dei programmatori nel caso in cui la macchina commetta dei danni.
L'obiettivo è quello di far luce sulle implicazioni etiche e legali del conferimento di una personalità elettronica ai robot, sostenendo che non è possibile far ciò senza generare contraddizioni. Inoltre, basandosi sulla difficoltà di determinare con precisione la responsabilità umana e robotica in un'azione, l'articolo suggerisce la creazione di un'assicurazione speciale che offra un risarcimento immediato.

The robot's status between juridical personality and responsibility

Nowadays, robots are used everywhere in our cities, workplaces and homes, constantly interacting with us. This paper delves into the question of whether a robot can be considered a legal person and analyzes the associated responsibilities that come with granting it such a recognition.
The discussion considers both the European and international juridical landscape, and follows two main paths. First, it investigates the concept of legal personhood, questioning whether it is appropriate to attribute it to a machine and how such a designation might be done. Secondly, it deals with the issue of accountability in the context of robotic actions, examining the potential responsibilities of robots, users, and programmers in case the machine commits damages. The aim is to shed light on the ethical and legal implication of conferring an electronic personality to robots, arguing that it is not possible without generating contradictions. Moreover, considering that it is difficult to precisely determine the human and robotic responsibility in an action, the article suggests the creation of a special insurance as a mean of immediate compensation.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 193-208

L'impiego della blockchain nel settore agroalimentare e l'approccio dell'Unione Europea

Mario Rafaniello*

Sommario: 1. Cenni introduttivi. – 2. L'utilità della blockchain nel settore agroalimentare. – 3. L'azione della Commissione europea. – 4. Il ruolo del Parlamento europeo. – 5. Conclusioni.

1. *Cenni introduttivi*

Negli ultimi anni la tecnologia blockchain, grazie alle proprie peculiarità e alla massiva digitalizzazione del mercato, si è progressivamente affrancata dal suo "luogo di nascita", cioè dal mondo delle cripto-valute, degli smart contract e delle attività finanziarie[1]; il suo l'impiego si è esteso fino ad abbracciare altri settori sia pubblici che privati. Una delle realtà produttive, che di recente ha visto accrescere la presenza della blockchain nelle strategie aziendali, è la filiera dell'agroalimentare, soprattutto in termini di tracciabilità e sicurezza[2]. Infatti, tra le citate peculiarità della blockchain vi sono caratteristiche utili in un mercato sempre più istantaneo, ramificato e globalizzato. Fattori come l'immodificabilità dei dati contenuti nei blocchi e la celerità con cui è possibile consultare e scambiare informazioni hanno consentito alla blockchain di attecchire in settori distanti dalle cripto-attività. Di questa tecnologia, appartenente al novero delle DLT (Distributed Ledgers Technology)[3], risulta arduo for-

* Dottorando di ricerca e Cultore della materia IUS/13 presso il Dipartimento di Scienze Politiche dell'Università degli Studi della Campania "Luigi Vanvitelli" di Caserta. Il suo oggetto di ricerca riguarda il rapporto tra *made in Italy* agroalimentare, ecosostenibilità e nuove tecnologie.

[1] Sulle origini della blockchain cfr. T. Gayvoronskaya, C. Meinel, *Blockchain. Hype Or Innovation*, Cham, Springer Nature Switzerland, 2021, pp. 5-6.

[2] Si precisa che questo contribuito tiene in considerazione la blockchain sotto tale profilo, tralasciando la sua originaria natura di strumento strettamente finanziario.

[3] Altra precisazione per le DLT, cui comunemente viene ascritta la blockchain. Secondo Finck, questo termine viene usato per indicare qualsiasi tipo di DLT, anche

nire una definizione univoca poiché non esistono ancora standard consolidati e, di conseguenza, in letteratura sono presenti diverse proposte[4]. Ad ogni modo, si può descrivere succintamente la blockchain come «un registro di contabilità condiviso e immutabile che facilita il processo di registrazione delle transazioni e la tracciabilità degli asset in una rete commerciale. Un asset può essere tangibile (una casa, un'auto, del denaro, dei terreni) o intangibile (proprietà intellettuale, brevetti, copyright, branding). Praticamente qualsiasi cosa che abbia un valore può essere rintracciata e scambiata su una rete blockchain, riducendo rischi e costi per tutte le parti coinvolte»[5]. In poche parole, la blockchain è un registro elettronico decentralizzato composto da blocchi di informazioni concatenati tra loro. Questi blocchi hanno la caratteristica di contenere, in generale, dati condivisibili, immutabili, crittografati e visibili ai membri della rete autorizzati[6] e sono ordinati cronologicamente consentendo, tramite l'esame della catena digitale, di poter ricostruire le vicende dell'informazione di riferimento.

Altro sarebbe utile condividere ma, chiariti almeno i tratti distintivi, si precisa che lo scopo del contributo è esaminare come la blockchain abbia ottenuto crescente spazio nel settore agroalimentare e in che modo l'Unione Europea – di seguito "UE" – si sia finora mossa nel tentativo di offrire una cornice normativa utile a sfruttarne le potenzialità.

quelle che non memorizzano i dati in blocchi. L'autore fa notare che, tecnicamente, le blockchain designano solo le varianti di DLT che registrano i dati in pacchetti concatenati ad altri. Cfr. M. Finck, "Blockchains and Data Protection in the European Union", «European Data Protection Law Review», vol. 4, n. 1, 2018, p. 18.

[4] S. Grima, M. Kizilkaya, K. Sood, M. ErdemDelice, "The Perceived Effectiveness of Blockchain for Digital Operational Risk Resilience in the European Union Insurance Market Sector", «Journal of Risk and Financial Management», vol. 14, n. 8, agosto 2021, pp. 2-4.

[5] Definizione fornita dalla IBM disponibile al link https://www.ibm.com/it-it/topics/blockchain.

[6] Solo i membri autorizzati possono accedere alle informazioni contenute in una blockchain, consentendo l'univocità delle informazioni. Il consenso all'aggiunta di informazioni è richiesto a tutti i membri della rete; una volta aggiunte, esse diventano immutabili, rafforzando la struttura della catena.

L'impiego della blockchain nel settore agroalimentare e l'approccio dell'Unione Europea

Il settore dell'agroalimentare è chiamato ad adattarsi alle sfide di quest'epoca, rappresentate dall'approvvigionamento energetico, dalla resilienza ai cambiamenti climatici, dalle variazioni della domanda e da un modello produttivo in fase di transizione verso la tanto richiesta ecosostenibilità. In tal senso, l'apporto fornito al settore dalle più recenti tecnologie, tra cui spicca la blockchain, è finora risultato indispensabile. L'Unione europea si è impegnata nel delineare un primo approccio normativo con l'intento di sfruttarne le potenzialità e favorire la competitività digitale del proprio mercato. Secondo alcuni, tuttavia, la blockchain potrebbe non essere la risposta a tutti i problemi del settore ma essa, se ben inquadrata, può fornire quella "spinta" innovativa che il Legislatore europeo auspica per il futuro.

The use of blockchain in the agri-food sector and the European Union approach

The agri-food sector is being called upon to adapt to the challenges of this era, represented by energy supply, resilience to climate change, variations in demand and a production model in transition towards much-needed eco-sustainability. In this sense, the contribution provided to the sector by the latest technologies, among which blockchain in particular stands out, has so far been indispensable. The European union has been busy outlining an initial regulatory approach with the intention of exploiting its potential and fostering the digital competitiveness of its market. According to some, however, blockchain may not be the answer to all problems in the sector, but it can, if properly framed, provide the innovative "push" that the european Legislator hopes for the future.

Ciberspazio e diritto, vol. 25, n. 76 (1 - 2024), pp. 209-232

Dato personale nella scoperta e nello sviluppo del farmaco *AI Driven*: basi, limiti, considerazioni

Gianluca rotino*

Sommario: 1. Premessa. – 2. La sperimentazione clinica nello sviluppo farmaceutico *AI Driven*. – 3. Basi giuridiche. La liceità del trattamento: primario e secondario. – 4. Limiti del consenso come base giuridica per i trattamenti multipli algoritmici. – 5. De-identificazione del dato personale. Cenni. – 6. Conclusioni.

1. *Premessa*

Uno degli aspetti della complessità del processo di scoperta e sviluppo del farmaco è l'innovazione, finalizzata a ridurre costi, tempi e, non da ultimo, rischi.

L'intelligenza artificiale (IA) viene applicata in ogni fase del processo, per migliorare design[1], efficacia, sicurezza, progettazione *de novo*, *repurposing* [2] e, persino, invenzione di composti mai osservati in natura[3].

* Fellow dell'ISLC-Information Society Law Center Università degli Studi di Milano. Consulente legale in diritto e strategia della innovazione, Data Governance and Protection, Cybersecurity, IP, Compliance Management systems. Esperto di aspetti giuridici delle applicazioni della IA e di diritto nella ricerca biomedica e nello sviluppo farmaceutico.

[1] Con il termine *drug design*, si indicano la progettazione e il design della molecola; l'esplorazione degli spazi chimico e biologico, inclusa, come si vedrà oltre; "l'invenzione" di composti (rif. proteine) del tutto nuove.

[2] La progettazione *de novo* (*de novo drug design*) è l'attività di progettazione di un farmaco del tutto nuovo, attraverso approcci sistematici su nuove ipotesi. Il *repurposing* (riqualificazione), detto anche *repositioning* (riposizionamento), invece, parte da un farmaco già approvato per il quale si indaga la possibilità di adozione per il trattamento di indicazioni diverse da quelle per cui si è ottenuta l'approvazione. Per una più dettagliata spiegazione cfr. M. Rudrapal et al., "Drug repurposing (DR): an emerging approach in drug discovery", in F.A. Badria (ed.), *Drug repurposing-hypothesis, molecular aspects and therapeutic applications*, vol.10, Londra, IntechOpen Ltd, 2020; V. D Mouchlis et al., "Advances in de novo drug design: from conventional to machine learning methods", «International journal of molecular sciences», vol. 22, n. 4, 2021, pp. 676 e ss.

[3] Per una recente panoramica della adozione della IA nella scoperta e sviluppo del farmaco cfr. C. Arnold, "Inside the nascent industry of AI-designed drugs", «Nature

I progressi delle scienze computazionali, insieme all'enorme e inedita disponibilità di dati, hanno determinato un profondo cambiamento nella scoperta e sviluppo del farmaco, in cui le applicazioni di intelligenza artificiale sono passate da un ruolo di mera assistenza a un ruolo di guida del processo: la *Pharma AI Driven*.

In ragione di questa prima considerazione, e anche per chiarezza e sintesi, non appare improprio dotare questa combinazione "sociotecnica"[4] di una autonomia disciplinare e coerenza di trattazione, definendo l'adozione dei sistemi di intelligenza artificiale nel processo di scoperta e sviluppo del farmaco con il termine di "algoraceutica"[5].

2. *La sperimentazione clinica nello sviluppo farmaceutico AI Driven*

Le attività algoraceutiche si fondano su un giacimento di dati composto in larga parte da una tipologia di dati che la *soft law* comunitaria

Medicine», vol. 29, n.6, 2023, pp.1292-1295; per l'applicazione della IA generative nell'invenzione di farmaci, cfr. https://www.technologyreview.com/2022/12/01/1064023/biotech-labs-are-using-ai-inspired-by-dall-e-to-invent-new-drugs/.

[4] Per sistema sociotecnico si intende una interazione di un sistema tecnologico, dedicato al processo di input-output, e un sistema sociale, gruppo relazionale che interagisce con la tecnologia. Definizione particolarmente adatta a descrivere il rapporto con la IA in contesti organizzativi complessi come quelli aziendali, in generale, e in quello dello sviluppo farmaceutico. Per una acuta analisi del sistema sanitario attuale come sistema sociotecnico e interessanti rinvii, cfr. F. Lagioia, *L'intelligenza Artificiale in sanità: un'analisi giuridica*, Torino, Giappichelli, 2020 pp. 47 e ss.

[5] Il termine "algoraceutica", qui proposto per descrivere questa applicazione della IA, è formato da *algor-*, abbreviazione di algoritmo, e *-aceutica*, abbreviazione di farmaceutica (come nel caso del termine nutri-ceutica, ad esempio). Al pari di termini come "algoretica" o "algocrazia", è un (proposto) neologismo, una parola "macedonia" (secondo la dizione della Accademia della Crusca), che sintetizza e cristallizza il rapporto emergente tra queste "DETs" (*Disruptive Emerging Technologies*) e il processo di sviluppo e produzione di medicinali che caratterizza l'evoluzione del settore.

Dato personale nella scoperta e nello sviluppo del farmaco AI Driven: basi, limiti, considerazioni

Questo Articolo esplora l'impatto dell'intelligenza artificiale (IA) nel settore farmaceutico, concentrandosi sull'adozione della cosiddetta algoraceutica, ovvero l'uso dell'IA nella scoperta e nello sviluppo di farmaci. Si evidenziano le implicazioni giuridiche della sperimentazione clinica condotta nell'ambito dell'AI Driven Pharma, con particolare attenzione alla raccolta e al trattamento dei dati personali, compresi quelli sensibili. Si discutono le basi giuridiche del trattamento dei dati, sia primario che secondario, e si esplorano i limiti del consenso come base giuridica per i trattamenti algoritmici multipli. Inoltre, si esamina l'importanza delle tecniche di de-identificazione del dato personale e le sfide legate alla protezione della privacy in un contesto in cui l'anonimizzazione potrebbe non essere più efficace. Infine, si sottolinea l'importanza di garantire un consenso informato e granulare, insieme a un chiaro dovere informativo da parte del titolare del trattamento, per tutelare adeguatamente i diritti e le libertà degli individui.

Personal data in AI Driven drug discovery and development: bases, limits, considerations

This Article explores the impact of artificial intelligence (AI) in the pharmaceutical industry, focusing on the adoption of so-called algoraceutic, or the use of AI in drug discovery and development. The legal implications of clinical trials conducted in AI Driven Pharma are highlighted, with a focus on the collection and processing of personal data, including sensitive data. The legal basis for data processing, both primary and secondary, is discussed, and the limitations of consent as a legal basis for multiple algorithmic treatments are explored. In addition, the importance of personal data de-identification techniques and the challenges related to privacy protection in a context where anonymization may no longer be effective are examined. Finally, the importance of ensuring granular informed consent, along with a clear duty of information on the part of the data controller, is emphasized in order to adequately protect the rights and freedoms of individuals.