Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 235-259

L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia "dato personale-non personale"

Carmine Andrea Trovato, Chiara Rauccio*

Sommario: 1. Introduzione. – 2. I concetti di "dato personale" e "anonimizzazione" nel GDPR. – 3. Il "fallimento" delle tradizionali tecniche di anonimizzazione. – 3.1. Gli attacchi ai dati personali e le tecniche di anonimizzazione. – 3.2. Il fallimento dell'anonimizzazione. – 4. I dati sintetici. – 4.1. Cosa sono i dati sintetici. – 4.2. L'inquadramento giuridico dei dati sintetici. – 4.3. I vantaggi dei dati sintetici. – 4.4. I rischi dei dati sintetici. – 5. Conclusione.

1. *Introduzione*

Ormai da diversi anni si sta assistendo al sempre più rapido sviluppo di sistemi di intelligenza artificiale che hanno ampliato la capacità di *data analysis* con finalità valutative e predittive[1]. Non c'è dubbio che uno sviluppo tecnologico di questo tipo produca una serie di vantaggi, soprat-

* Carmine Andrea Trovato è consigliere giuridico della vicepresidente del Garante per la protezione dei dati personali. In passato, ha svolto l'attività di consulente privacy presso studi legali nazionali e internazionali. È inoltre docente di numerosi corsi e LL.M. in diritto delle nuove tecnologie e data politics.

Chiara Rauccio è consulente privacy in-house dopo aver maturato una significativa esperienza presso uno studio legale, assistendo società nazionali e internazionali in materia di protezione dei dati personali. Dopo la laurea in giurisprudenza ha conseguito l'abilitazione alla professione forense e ha svolto un LL.M. in Law & Technology e numerosi corsi di perfezionamento in materia.

[1] Cfr. P. Stone, R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus, K. Leyton-Brown, D. Parkes, W. Press, A. L. Saxenian, J. Shah, M. Tambe, A. Teller, "Artificial Intelligence and Life in 2030", «One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University», Stanford, CA, settembre 2016; Ulster University, Cognitive Analytics Research Lab, "Cognitive Analytics – Combining Artificial Intelligence (AI) and Data Analytics", disponibile al link https://

tutto in ambiti quali la ricerca, la medicina, la sostenibilità. Tuttavia, possono derivarne anche dei rischi, soprattutto quando a essere in gioco sono i dati personali, ossia informazioni collegabili direttamente o indirettamente a persone fisiche. In questo caso, un utilizzo non corretto può produrre conseguenze pregiudizievoli per i diritti e le libertà non solo dei soggetti a cui i dati si riferiscono, ma della società in generale, ad esempio nel caso di decisioni assunte nei confronti di gruppi di individui sulla base di analisi condotte da sistemi di intelligenza artificiale[2].

Questa compresenza di vantaggi da un lato e rischi dall'altro ha reso necessario trovare un punto di equilibrio che consenta di tutelare tutti gli interessi in gioco, bilanciando le diverse esigenze della società, talvolta in contrasto tra loro[3]. Da questo punto di vista ha assunto un ruolo centrale il Regolamento UE 2016/679 in materia di protezione dei dati personali ("Regolamento" o anche "GDPR")[4]. Già l'art. 1(1) chiarisce che la finalità del Regolamento è di stabilire «norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati»[5]. Questa impostazione è confermata nei primi Considerando, in cui il Legislatore europeo ha voluto chiarire come lo scopo del Regolamento non sia quello di impedire o limitare il trattamento dei dati personali ma, al contrario, di creare uno spazio di libertà, sicurezza e giustizia, in cui sia garantito il rafforzamento delle economie nel mercato interno e il benessere delle persone fisiche[6]. In

www.ulster.ac.uk/cognitive-analytics-research/cognitive-analytics (ultimo accesso in data 13 giugno 2022).

[2] Cfr. S. Wachter, "The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law", «Tulane Law Review», febbraio 2022, Forthcoming.

[3] Si pensi, ad esempio, ai sistemi di IA utilizzati per la videosorveglianza di massa o il riconoscimento facciale e all'impatto che essi possono avere sui diritti e le libertà delle persone. Sul tema del rapporto tra dimensione individuale e collettiva nella società dei *big data* cfr. B. van der Sloot, "The Individual in the Big Data Era: Moving towards an Agent-Based Privacy Paradigm" in B. van der Sloot, D. Broeders, E. Schrijvers (eds), *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, pp. 177-203.

[4] Cfr. 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).

[5] Cfr. Art. 1, par. 1, GDPR.

[6] Cfr. Considerando 4 GDPR.

L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia "dato personale-non personale"

Nell'attuale data economy la raccolta e l'analisi dei dati assume un ruolo centrale. Tuttavia, quando oggetto di tali attività sono i dati personali, le esigenze economiche devono essere contemperate con la necessità di rispettare la normativa in materia di protezione dei dati personali, normativa che non trova invece applicazione con riferimento ai dati anonimi. Per questo motivo nel corso degli ultimi anni è diventato sempre più determinante il ricorso a tecniche di anonimizzazione che, da un lato, eliminino ogni indicatore riconducibile a una persona fisica, ma dall'altro mantengano l'utilità statistica delle informazioni. Mentre finora tale obiettivo non sembra essere stato raggiunto, si sta recentemente affermando una nuova tecnica, c.d. *data synthesis*, che potrebbe rappresentare uno strumento particolarmente utile in tal senso. Il presente articolo si propone dunque di analizzare i dati sintetici, esaminandone i potenziali vantaggi ma anche i limiti e i rischi che potrebbero derivare dal loro utilizzo.

Is anonymization dead? An analysis of synthetic data as a proposal to overcome the "personal-non-personal data" dichotomy

Collecting and analysing data plays a crucial role in today's data economy. However, when the processing relates to personal data, economic needs must be balanced with the requirement to comply with the personal data protection legislation. On the contrary, such a legislation does not apply to anonymous data. As such, over the last few years scientific research has been struggling for finding anonymization techniques that delete any personal identifier but, at the same time, preserve information statistical utility. The measures used so far seem to have not reached such a goal but a new emerging technique, "data synthesis", might offer major results. Thus, the present article aims at examining synthetic data in order to pin down its opportunities but also the risks it could pose.

Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 261-279

Ruoli soggettivi in materia di certificazione nell'ambito della normativa sulla privacy

Massimo Cardi*

Sommario: 1. Premessa. – 2. Il Garante per la protezione dei dati personali. – 3. Accredia. – 4. I rapporti tra Accredia e il Garante. – 5. Gli Organismi di certificazione. – 6. I requisiti aggiuntivi di accreditamento degli enti di certificazione. – 7. I meccanismi di certificazione e i criteri. – 8. Conclusioni.

1. *Premessa*

La Direttiva 95/46/CE è stata per anni punto di riferimento della normativa dell'Unione europea in materia di protezione dei dati personali. Nata, però, in un contesto tecnologico ormai superato, è stata abrogata e sostituita dal nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento UE n. 2016/679), entrato in vigore il 24 maggio 2016 (GDPR)[1]. Esso si articola in 11 Capi per un totale di 99 articoli, preceduti da 173 Considerando, aventi il compito di chiarire le ragioni e il contesto della nuova normativa.

* Lead Auditor certificato AICQ Sicev negli schemi Qualità, Ambiente e Sicurezza. Ha frequentato il Corso di Alta Formazione in Data Protection e Privacy Officer all'Università di Bologna.

[1] Per un commento al Regolamento europeo, cfr. G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019; S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, CEDAM, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Vol. I (Dalla Direttiva 95/46 al nuovo Regolamento europeo) e Vol. II (Il Regolamento europeo 2016/679), Torino, Giappichelli, 2016; C. Bistolfi, L. Bolognini, E. Pelino, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016.

All'interno del Regolamento sono state inserite diverse misure aventi il compito di facilitare la conformità alle disposizioni del GDPR, tra cui requisiti obbligatori in circostanze specifiche, nonché misure volontarie, quali codici di condotta e meccanismi di certificazione[2].

In particolare, il Regolamento ha introdotto, agli articoli 42 e 43, dei meccanismi di certificazione che consentono di dimostrare la conformità alle sue prescrizioni o, in altre parole, di aderire a quel principio di *accountability* che risulta essere alla base del Regolamento stesso. Recita, infatti, l'articolo 42 che «Gli Stati membri, le Autorità di controllo, il Comitato e la Commissione incoraggiano […] l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese».

L'articolo 42, comma 1, richiama alcuni elementi fondamentali che sono stati successivamente analizzati e interpretati dalle Linee Guida EDPB 1/2018[3]. Gli Stati membri hanno il compito di incoraggiare l'istituzione di meccanismi di certificazione, i quali possono incrementare la trasparenza non solo per gli interessati ma, anche, nelle relazioni tra le imprese. A tale riguardo, è stato rilevato che «La certificazione, pertanto, quale atto volontario, ha il fine ultimo complessivo di infondere fiducia, a tutte le parti interessate, che un prodotto soddisfi i requisiti specificati. Il valore della certificazione, quindi, è il grado di fiducia e di credito stabilito da un'imparziale e competente dimostrazione del soddisfacimento di requisiti specificati, effettuata da una terza parte»[4].

[2] Cfr. European Data Protection Board (EDPB), *Linee Guida 4/2018 relative all'accreditamento degli Organismi di certificazione ai sensi dell'articolo 43 del Regolamento generale sulla protezione dei dati (2016/679*), versione 3.0, 4 giugno 2019, par. 1.

[3] Cfr. European Data Protection Board (EDPB), *Linee Guida 1/2018 relative alla certificazione e all'identificazione dei criteri di certificazione in conformità degli articoli 42 e 43 del Regolamento (UE) 2016/679*, cit., par. 1-14.

[4] Cfr. R. Giannetti, *Certificazione GDPR, un'altra certificazione,* documento disponibile su Internet all'indirizzo https://www.in-veo.com/it/107-blog-it/487-certificazione-gdpr-un-altra-certificazione-it#_ftn1 (consultato da ultimo in data 1° maggio 2021).

Ruoli soggettivi in materia di certificazione nell'ambito della normativa sulla privacy

L'articolo si occupa di analizzare i soggetti coinvolti dalla normativa privacy, in particolare dagli articoli 43 e 44 del GDPR, che hanno introdotto dei meccanismi di certificazione che consentono di dimostrare la conformità alle sue prescrizioni o, in altre parole, di aderire a quel principio di accountability che risulta essere alla base del Regolamento stesso.

Subjective roles in certification under privacy law

The article analyses the subjects involved in the privacy legislation, in particular Articles 43 and 44 GDPR, which have introduced certification mechanisms to demonstrate compliance with its requirements or, in other words, to adhere to the principle of accountability that underlies the Regulation itself.

Informatica Giuridica e Società Tecnologica

Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 283-295

I *transborder data access*: analisi dell'articolo 32 della Convenzione di Budapest

Gaia Brino Bet [*]

Sommario: 1. Premessa. – 2. Introduzione ai transborder data access. – 2.1. Cybercrime Convention Committee. – 2.2. Problematiche rilevate dall'Explanatory Report. – 2.3. Articolo 32a. Accesso transfrontaliero ai dati pubblicamente disponibili. – 2.4. Articolo 32b. Accesso transfrontaliero che necessita del consenso. – 2.4.1. Cosa si intende per "accesso transfrontaliero" e "dati informatici memorizzati in un altro Stato"? – 2.4.2. Cosa si intende per "Accesso senza l'autorizzazione dell'altra Parte"? – 2.4.3. In cosa consiste il consenso? – 2.4.4. Quale legge si applica? – 2.4.5. Chi è la persona che può fornire l'accesso o divulgare i dati? – 2.4.6. Dove si trova la persona quando acconsente a fornire o quando fornisce l'accesso?

1. *Premessa*

Per cyberspace si intende un "non" territorio, un luogo impalpabile che conduce a rivisitare tutta la disciplina troppo attaccata al concetto di materialità. Ebbene, lo spazio virtuale non esiste, il cloud di per sé non è un mondo virtuale e parallelo, poiché ogni cloud è collocato su un server ed ogni server ha un indirizzo ricollegabile ad uno spazio terreno. Quella in esame è una questione tra le più antiche regolate dal diritto internazionale, che attira l'attenzione già dal 1700 con Jeremy Bentham riguardo al problema del conflitto tra giurisdizioni statali in materia penale[1]; tale tema concerne il diritto penale e processuale penale internazionale e, pur riguardando fattispecie online, non necessita di categorie *ad hoc*.

Teoricamente, procedendo con un'esemplificazione dell'argomento in analisi, se l'Autorità giudiziaria è a conoscenza dell'indirizzo di un ser-

[*] Dottoressa in Giurisprudenza.

[1] Cfr. J. Bentham, *An introduction to the Principles of Moral and Legislation*, Oxford, Oxford Clarendon Press, 1789.

doi 10.53148/CD202202003

ver contenente dati utili può procedere direttamente alla perquisizione nel suolo nazionale oppure può inoltrare la richiesta di tali dati se si trovano all'estero e, per il buon funzionamento delle indagini, di fondamentale importanza è la collaborazione con i gestori dei server, che sono sempre a conoscenza dell'allocazione dello stesso. Il punto non è dove sono conservate le informazioni, bensì quali strumenti di acquisizione possono essere utilizzati per recepire dati telematicamente accessibili anche dal territorio nazionale.

In quanto al concetto di giurisdizione si distinguono diverse categorie:

i) *jurisdiction to prescribe*: che identifica la competenza a regolamentare giuridicamente una fattispecie;
ii) *jurisdiction to adjudicate*: che coincide con il potere di dirimere le controversie;
iii) *jurisdiction to enforce*: che riguarda la titolarità del potere di garantire l'attuazione coattiva delle decisioni;
iv) *jurisdiction to investigate*: una parte della dottrina ha suggerito di aggiungere, con riguardo alle indagini informatiche tale categoria, retta da criteri, logiche e condizioni di titolarità differenti ed autonome rispetto alle altre[2].

2. *Introduzione ai transborder data access*

Vista la complessità di questa nuova forma di reati, gli Stati, durante la Convenzione di Budapest del 2001, hanno sentito l'esigenza di instaurare una mutua assistenza relativa ai poteri di indagine per la trasmissione e l'acquisizione di dati informatici, immagazzinati in computer allocati in Paesi differenti. Questa branca, definita "transborder data access", viene disciplinata dalla sezione II Titolo II Conv. 2001, che consta di quattro articoli. L'articolo più importante e controverso è il trentaduesimo, intitolato "Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili"; secondo tale artico-

[2] Cfr. F. Cajani, G. Cernuto, G. Costabile, F. D'Arcangelo, *Le nuove frontiere dell'acquisizione degli elementi di prova nel cyberspazio*, Milano, IISFA, 2017; G.M. Ruotolo, *Il transborder data access tra obblighi internazionali e norme interne di adattamento*, Milano, IISFA, 2016.

I transborder data access: analisi dell'articolo 32 della Convenzione di Budapest

Il conflitto tra giurisdizioni statali in materia penale è una questione tra le più antiche regolate dal diritto internazionale e, con l'entrata in scena dei cybercrimes, la problematica è diventata sempre più intensa. Durante la Convenzione di Budapest, nel 2001, si è cercato di delineare l'argomento riguardante i *transborder data access*, di modo da creare una *Mutual Legal Assistance* tra gli Stati nella ricerca e raccolta del materiale utile per formulare un'imputazione. Il fine era quello di rendere il procedimento più semplice, veloce ed efficiente, ma l'intervento, invece che risolvere il problema, ha creato ancora più incomprensioni.

Transborder data access: analysis of Article 32 of the Budapest Convention

One of the oldest issues regulated by international law concerns the conflict between State jurisdictions in criminal matters and with the arrival of cybercrimes the problem has become increasingly intense.
During the Convention of Budapest that took place in 2001, the participating states tried to create a proper discipline regarding transborder data access, in order to develop Mutual Legal Assistance between the States on the research and collection of useful material for formulating an indictment.
The aim was to create a simpler, faster, and more efficient procedure, but the intervention, instead of solving the problem, created even more misunderstandings.

Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 297-310

L'intelligenza artificiale per la "Green Sustainability"

Paulina Kowalicka*

Sommario: 1. Introduzione. – 2. Strategie politiche. – 2.1. "2030 Digital Compass: the European way for the Digital Decade". – 2.2. *Green Deal* europeo. – 3. Tra innovazione sostenibile e sostenibilità innovativa. – 4. Conclusioni.

1. *Introduzione*

Nel pieno della crisi ambientale, energetica e di materie prime che il mondo sta vivendo, il concetto di sostenibilità ha assunto maggiore importanza e la società ha acquisito una più ampia consapevolezza in merito. Nonostante la recente aggressione militare russa contro l'Ucraina abbia comportato implicazioni a lungo termine al settore dell'energia, alimentare, all'economia, alla sicurezza, alla difesa e alla geopolitica, il percorso dell'Europa verso il raggiungimento di transizioni verdi e digitali ha subito una forte accelerata, messo alle strette da una situazione al limite del pronosticabile. Se la digitalizzazione rappresenta da anni un processo inarrestabile, intrapreso dai più importanti Paesi europei, oggi occorre riscrivere la strada tracciata solo pochi anni fa, per fare spazio al tema della sostenibilità.

Digitalizzazione e sostenibilità sono, attualmente, i principali temi dell'agenda politica dell'UE e si pensa che la loro interazione possa avere enormi conseguenze per il futuro. Sebbene siano di natura diversa e ciascuna soggetta a dinamiche specifiche, il loro *gemellaggio*, ovvero la capacità di rafforzarsi a vicenda, risulta fondamentale per le politiche di innovazione. La transizione verde non avverrà senza gli obiettivi e le politiche stabilite nel *Green Deal europeo*, una strategia trasversale per raggiungere la neutralità climatica e ridurre la crisi ambientale entro il

* Assegnista di ricerca in Informatica giuridica presso il Dipartimento di Scienze giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano e Research Fellow dell'ISLC - Information Society Law Center.

doi 10.53148/CD202202004

2050[1]. Fino a poco tempo fa, la transizione digitale è progredita con solo considerazioni di sostenibilità limitate: per ridurre gli effetti collaterali negativi e sfruttare appieno il suo potenziale consentendo la sostenibilità ambientale, sociale ed economica, l'evoluzione digitale richiede un'adeguata e puntuale definizione delle politiche e governance.

«Per raggiungere la neutralità climatica entro il 2050 dobbiamo liberare il pieno potenziale della digitalizzazione e, allo stesso tempo, mettere la sostenibilità al centro della trasformazione digitale. È per questo che la relazione di previsione strategica esamina in modo più approfondito come allineare al meglio i due obiettivi, soprattutto alla luce dell'importanza che assumono in termini di sicurezza nel mutato contesto geopolitico attuale. A partire dal 2040, ad esempio, il riciclaggio potrebbe essere una fonte importante di metalli e minerali, essenziali per le nuove tecnologie, se l'Europa vorrà porre rimedio alle sue carenze nel settore delle materie prime. Comprendere l'interazione tra le due transizioni adoperandosi, nel contempo, per conseguire un'autonomia strategica aperta, è la giusta via da seguire»[2].

2. *Strategie politiche*

Al fine di raggiungere l'obiettivo prescritto, è necessario investire su una adeguata ed efficiente definizione delle strategie, delle politiche e della governance, in termini di transizione digitale e sostenibilità, affinché si possa ridurre l'impatto negativo e potenziare il quadro ambientale, sociale ed economico.

[1] Cfr. Communication from the Commission to the European Parliament and the Council, "2022 Strategic Foresight Report, Twinning the green and digital transitions in the new geopolitical context", COM (2022) 289 final, Brussels 29.6.2022, disponibile al seguente indirizzo Internet: https://ec.europa.eu/info/files/strategic-foresight-report-2022_en. (Consultato a luglio 2022).

[2] Maroš Šefčovič, vicepresidente della Commissione europea e Commissario europeo per l'unione energetica dal 2014.

L'intelligenza artificiale per la "Green Sustainability"

Nel nuovo contesto geopolitico, uno degli obiettivi principali dell'Unione europea è conciliare l'innovazione tecnologica e la tutela dell'ambiente per favorire un progresso più sostenibile e un nuovo modello economico. Il gemellaggio tra innovazione sostenibile – digital – e sostenibilità innovativa – green – rappresenta il punto di partenza per contribuire al reciproco sviluppo, guidare il progresso e adattare le strategie politiche e sociali dell'UE, sostenendo una nuova economia, circolare e climaticamente neutra, ripristinando la biodiversità e riducendo i livelli di emissioni inquinanti, attraverso l'utilizzo di tecnologie d'avanguardia. Lo scopo è favorire l'impatto positivo e mitigare l'impatto negativo dell'intelligenza artificiale sull'ambiente e di conseguenza sulle persone e sui profitti.

Artificial Intelligence for Green Sustainability

In the new geopolitical context, one of the main objectives of the European Union is to reconcile technological innovation and environmental protection to promote more sustainable progress and a new economic model. The twinning of sustainable innovation – digital – and innovative sustainability – green – is the starting point for contributing to mutual development, driving progress and adapting EU political and social strategies by supporting a new, circular and climate-neutral economy, restoring biodiversity and reducing pollutant emission levels, through the use of cutting-edge technologies. The aim is to foster the positive impact and mitigate the negative impact of artificial intelligence on the environment and consequently on people and profits.

Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 311-333

Prospettive e recenti sviluppi della tutela dei minori online

Giulia Pesci*

Sommario: 1. Introduzione, il minore online. – 2. Le novità introdotte dal *Digital Services Act*. – 3. Nuove norme in materia di *Child Sexual Abuse Material* (CSAM) online. – 4. Le ultime proposte di intervento italiane a tutela dei diritti dei minori in rete.

1. *Introduzione, il minore online*

Negli ultimi anni, con gli sviluppi ormai noti della rete, dei social network, dei sistemi di messaggistica istantanea e dell'*Internet of Things*, la figura del minore è al centro dei dibattiti in materia di sicurezza e uso responsabile della tecnologia.

I minori vengono spesso, infatti, considerati, da un lato, come soggetti particolarmente vulnerabili ai quali prestare attenzione per quanto concerne tutte le tematiche che riguardano il ciberspazio; dall'altro lato, come i principali destinatari di progetti di educazione e responsabilizzazione nei confronti delle "nuove" tecnologie.

È ormai risaputo che un bambino o un ragazzo che si trovi a interagire – tra l'altro sempre più precocemente – online può incorrere in diversi rischi o pericoli, alcuni particolarmente gravi e in grado di mettere a rischio la sua sicurezza e la sua salute fisica e mentale. Per questa ragione, si registra un costante incremento di attenzione nei confronti del fenomeno da parte delle istituzioni, della società civile, delle Forze di polizia, delle aule di giustizia e dei Legislatori.

Nonostante l'impegno internazionale e trasversale volto alla tutela dei minori online, non si può fare a meno di evidenziare quanto il dirit-

* Assegnista di ricerca in Informatica giuridica presso il Dipartimento di Scienze giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano e Research Fellow dell'ISLC - Information Society Law Center.

doi 10.53148/CD202202005

to, e i processi di regolamentazione in generale, fatichino ancora a stare al passo degli inarrestabili e sempre più rapidi sviluppi tecnologici.

Per riportare un esempio concreto di quanto si sta affermando, in diversi Stati europei e del resto del mondo, i Legislatori hanno previsto dei precisi limiti di età per l'accesso alle piattaforme o ai social network; tuttavia, risulta chiaramente visibile quanto la questione sia complessa da gestire dal punto di vista pratico.

Il numero di bambini e bambine che interagiscono online, sovente senza alcun tipo di controllo da parte delle figure adulte di riferimento, è in costante aumento e la soglia di età dei primi accessi a Internet da parte degli stessi registra una continua diminuzione.

In Italia, ad esempio, il minimo di età previsto per esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione è stato fissato a quattordici anni dal d.lgs. 10 agosto 2018, n. 101, in attuazione dell'articolo 8 del GDPR.

Nonostante questo limite, e nonostante il limite di età previsto da diverse piattaforme, al di sotto del quale gli utenti non potrebbero iscriversi e accedervi, basta frequentare i social network più celebri per rendersi conto di quanto, nel concreto, tali limiti non vengano rispettati. Senza entrare nel merito della questione, un altro elemento chiave e che desta particolare allarme in tema è la cronaca che coinvolge bambini e bambine sempre più piccoli, ad esempio, in relazione alle *challenge* online che talvolta mettono a rischio la loro vita, oppure in relazione ai casi di adescamento che si verificano in rete.

2. *Le novità introdotte dal* Digital Services Act

Nel contesto delle misure volte a rendere Internet uno spazio più sicuro per i cittadini europei, l'Unione europea, da tempo, si dedica con particolare attenzione alla sicurezza dei minori online, mediante una serie di interventi legislativi e attività di informazione e sensibilizzazione.

Verso la fine del 2020, infatti, la Commissione europea ha elaborato e presentato un «pacchetto sui servizi digitali» e, nello specifico, la legge sui servizi digitali, nota come *Digital Services Act*, che riassume l'obiettivo dell'Unione europea di sviluppare «una novità mondiale nel campo della

Prospettive e recenti sviluppi della tutela dei minori online

Negli ultimi anni, la figura del minore è al centro dei dibattiti in materia di sicurezza e uso responsabile della tecnologia e tali dibattiti si mostrano sempre più complessi in ragione dei costanti e inarrestabili sviluppi della rete, dei social network, dei sistemi di messaggistica istantanea e dell'*Internet of Things*.
Nel presente Articolo sono analizzate alcune nuove proposte che intervengono direttamente o in modo trasversale in materia di tutela dei minori online, affrontando le diverse problematiche e i rischi che li coinvolgono.

Perspectives and recent developments in online child protection

In recent years, minors are at the center of debates regarding the safety and responsible use of technology, and these debates are showing themselves to be increasingly complex due to the constant and unstoppable developments in the Internet, social networks, instant messaging systems, and the Internet of Things.
This Article analyzes some new proposals that deal with the protection of minors online, addressing the various issues and risks involving them.

Ciberspazio e diritto, vol. 23, n. 71 (2 - 2022), pp. 335-349

Il mercato unico digitale e il nuovo assetto di tutele che attende il consumatore

Claudia Ogriseg*

Sommario: 1. Il potenziamento del mercato unico digitale: il "New Deal for Consumers" grazie alle Direttive UE n. 2019/770, n. 2019/771, n. 2019/2161 e n. 2020/1828. – 2. L'estensione della protezione del consumatore in caso di cessione dei dati personali nella fornitura di contenuti digitali. – 3. I rimedi e le tutele garantite ai consumatori digitali. – 4. Le modifiche al Codice del consumo italiano introdotte dalla normativa di recepimento delle Direttive UE n. 2019/770 e n. 2019/771. – 5. I Regolamenti approvati e in discussione a livello europeo per un "New Deal" di tutele nel mercato unico digitale.

1. *Il potenziamento del mercato unico digitale: il "New Deal for Consumers" grazie alle Direttive UE n. 2019/770, n. 2019/771, n. 2019/2161, n. 2020/1828*

Sfumato il tentativo di uniformare le regole della vendita con la proposta di regolamento per un diritto comune europeo (CESL), l'Unione europea ha emanato un "pacchetto" di Direttive che è stato considerato un vero e proprio "New Deal for Consumers"[1]. Si tratta della Direttiva UE n. 2019/770 sui contratti di fornitura di contenuti e servizi digitali, della Direttiva UE n. 2019/771 sui contratti di vendita inclusi i beni con elementi digitali, della Direttiva UE n. 2019/2161 c.d. "Direttiva omnibus" poiché interviene su ambiti eterogenei relativi a contratti tra professionisti e consumatori e della Direttiva UE n. 2020/1828 sulle azioni rappresentative per la tutela degli interessi collettivi dei consumatori.

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

[1] Cfr. S. Perugini, *La normativa comunitaria*, in G. Cassano, M. Dona, R. Torino, *Il diritto dei consumatori*, Milano, Giuffré, 2021, p. 27 e sul punto p. 45 e ss.

L'obiettivo perseguito con questo primo "pacchetto" di Direttive è stato il potenziamento nell'Unione di un autentico mercato unico digitale in cui la disciplina della vendita di beni e della fornitura di contenuti e servizi digitali siano armonizzate[2]. L'esigenza di una disciplina comune sui contratti di fornitura di contenuti e/o servizi digitali è stata perseguita con Direttive con un ridotto margine di intervento agli Stati membri in fase di recepimento, finalizzate a un incremento delle tutele per i consumatori. È questo il motivo per cui si è parlato di un "New Deal for Consumers". Le norme euro-unitarie qui richiamate hanno codificato l'esigenza di una maggior trasparenza nel mercato digitale, hanno esteso le protezioni per il consumatore anche in caso di contratti gratuiti e hanno previsto il diritto al risarcimento per le vittime di pratiche commerciali ingiuste, oltre a prescrivere agli Stati membri l'introduzione di sanzioni effettive, proporzionate e dissuasive anche promuovendo una *class action* europea.

Analizzando più nel dettaglio il contenuto di queste discipline si osserva come la Direttiva UE n. 2019/770 regoli i contratti di fornitura di contenuti e servizi digitali. La finalità è quella di proteggere i consumatori negli scambi commerciali di programmi informatici, applicazioni, file video, audio, giochi digitali, libri elettronici, servizi digitali per la creazione e archiviazione dei dati, software per la condivisione di file, *file hosting,* videoscrittura, servizi su cloud e social media[3]. Si introducono tutele per il consumatore rispetto a "operatori economici" ossia qualsiasi persona fisica o giuridica, indipendentemente dal fatto che si tratti di un soggetto pubblico o privato, che agisca per finalità che rientrano nel qua-

[2] Cfr. G. Capilli, "Le direttive 2019/770/UE, 2019/771/UE e 2019/2161: verso l'unificazione (salvo deroghe) della disciplina sulla tutela dei consumatori nel mercato digitale", «Diritto di internet», 30 gennaio 2020, https://dirittodiinternet.it/7664-2/.

[3] La Direttiva UE n. 2019/770 introduce una regolamentazione per «contenuti digitali», ovvero i dati e prodotti forniti in formato digitale (*i.e.* programmi informatici, applicazioni, *file* video/audio/musicali, giochi digitali, libri elettronici, cfr. art. 2 par. 1 n. 1), «servizi digitali» ovvero servizi che consentono al consumatore di creare, trasformare, archiviare dati o accedervi in formato digitale o consentono la condivisione o qualsiasi altra interazione con tali dati (*i.e*. software che permettono creazione/trasformazione/condivisione/archiviazione di audio e video, giochi offerti nell'ambiente di *cloud computing* art. 2 par. 1, n. 2).

Il mercato unico digitale e il nuovo assetto di tutele che attende il consumatore

Nel presente articolo si delinea l'assetto di regole introdotte a tutela del consumatore nel mercato digitale in tema di vendita e fornitura di beni e servizi digitali con le Direttive UE n. 2019/770 e n. 2019/771. L'attenzione è focalizzata sulla protezione garantita in caso di cessione dei dati personali effettuata *a latere* di una fornitura digitale e sui rimedi previsti in generale per il consumatore digitale.

The single digital market and the new set of protections that awaits the consumer

The paper outlines the set of rules introduced to protect the consumer in the digital market in terms of the sale and supply of digital goods and services set out in EU Directives 2019/770 and 2019/771. The attention is focused on the protection guaranteed in the event of the transfer of personal data carried out on the sidelines of a digital supply and on the remedies provided to the digital consumer.