Diritto e politica dei trasporti

Rivista semestrale *open access* di dottrina, giurisprudenza e documentazione

Fascicolo 2/2024

Con i contributi di
Andrea De Lia, Francesco Tomasicchio, Gabriele Pisanti, Maria Pia d'Antuono, Maria Lavalle, Antonio Cecere, Federica D'Andrea, Emma Maresca, Roberta Brignoccolo

ISSN 2612-5056

LUISS

La Rivista è pubblicata dall'Osservatorio sul Trasporto Aereo "Antonio Catricalà" della Luiss G. Carli, ed è registrata presso il Tribunale di Roma al n. 150/2018 del 19 settembre 2018.
The Journal is published by the Air Transport Observatory "Antonio Catricalà" at Luiss G. Carli, and it is registered at the Court of Rome under No. 150/2018 on 19 September 2018.
Direttore responsabile/Editor-in-Chief: Prof. Francesco Gaspari, Università degli Studi "G. Marconi" di Roma e Osservatorio sul Trasporto Aereo "Antonio Catricalà" Luiss G. Carli
http://www.dirittoepoliticadeitrasporti.it/
La rivista è promossa dall'Osservatorio sul Trasporto Aereo "Antonio Catricalà" Luiss G. Carli, anno 7, n. 12 (I-2024)

ISSN 2612-5056
Luiss University Press

Diritto e politica dei trasporti è una Rivista online e open-access, classificata dall'Anvur tra le riviste di classe A nell'area disciplinare 12 (Scienze giuridiche), indicizzata da DOAJ – Directory of Open Access Journals (https://doaj.org/) e da ERIH PLUS – European Reference Index for the Humanities and Social Sciences (https://kanalregister.hkdir.no).
Diritto e politica dei trasporti is an online,open-access, Anvur class A Journal, subject area 12 (Law). It is indexed in DOAJ – Directory of Open Access Journals (https://doaj.org/) and in ERIH PLUS – European Reference Index for the Humanities and Social Sciences (https://kanalregister.hkdir.no).

Grafica e impaginazione: Ente Nazionale Aviazione Civile e Luiss University Press
Pubblicato nel mese di febbraio 2025

Modalità di invio dei contributi
Chiunque può inviare il suo scritto in file ".doc" alla direzione della Rivista (direzione@dirittoepoliticadeitrasporti.it) o alla Segreteria editoriale (redazione@dirittoepoliticadeitrasporti.it) unitamente alle seguenti informazioni:
1) i dati personali dell'Autore, la qualifica accademica e/o professionale, nonché i recapiti;
2) un abstract in lingua inglese e uno in lingua italiana, che non deve superare le 1.000 battute ciascuno (spazi inclusi), 5 parole chiave;
3) l'autorizzazione al trattamento dei dati personali forniti dall'Autore alla Rivista, ai sensi del Regolamento UE 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016 (Regolamento Generale sulla Protezione dei Dati), nonché del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);
4) una formale richiesta di pubblicazione, che si intende implicitamente inclusiva delle seguenti dichiarazioni da parte dell'Autore:
a) che il lavoro sia esclusivo frutto dell'Autore e sia stato redatto nel rispetto delle norme del diritto d'autore e della riservatezza delle informazioni anche con riferimento alle fonti utilizzate;
b) che l'Autore non ha già pubblicato ovvero non ha chiesto la pubblicazione dello scritto ad altra rivista, salvo espresso consenso del Direttore o del Comitato di direzione;
c) che le posizioni espresse impegnano l'Autore e non la Rivista;
d) che l'Autore esonera la Rivista da ogni responsabilità con riguardo alla scelta di pubblicare lo scritto, non pubblicarlo o di rimuoverlo dalla rivista in caso di violazione di norme di legge o nei casi previsti dal Codice etico adottato dalla Rivista;
e) che l'Autore rispetta tutte le altre indicazioni contenute nel Codice etico della Rivista.
Il Direttore o il Comitato di direzione si riserva di non pubblicare i contributi che non rispettino le caratteristiche editoriali richieste. Gli autori sono gli unici responsabili dei contenuti dei loro scritti. Non si accettano scritti anonimi.
Tutti i contributi sono pubblicati in formato PDF. Si possono stampare gli "estratti" con le indicazioni tipografiche della Rivista e con la data di pubblicazione.
I criteri redazionali sono indicati nell'apposita sezione della Rivista.

Submission of contributions
Manuscripts are sent in ".doc" format to the Journal's Executive Editors (direzione@dirittoepoliticadeitrasporti.it) or to the Editorial Staff (redazione@dirittoepoliticadeitrasporti.it). The e-mail includes the following information:
1) Author's personal data, academic and/or professional qualifications, contacts;
2) an abstract in Italian language and an abstract in English of not more than 1.000 characters each (including spaces), 5 key words;
3) authorization to process personal data provided by the Author to the Journal in accordance with Regulation EU 679/2016 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), and Legislative Decree 30 June 2003, No. 196 (Italian Personal Data Protection Code);
4) request to publish the manuscript, which implicitly includes the following declarations by the Author:

a) that the manuscript is the result of research activity conducted by the Author and that it complies with the rules on intellectual property rights and on confidentiality of information, also with regards to the sources used;
b) that the manuscript has not been already published nor has been submitted for publication to another Journal, except for express consent by the Editor-in-Chief or the Executive Editors;
c) that the views expressed in the publication are the sole responsibility of the Author and do not reflect the views of the Journal;
d) that the Author explicitly exonerates the Journal of all responsibility with regards to the choice to publish the manuscript, not to publish it, as well as to remove it from the Journal in the event of a breach of any legal provisions or in the cases laid down in the Code of Ethics adopted by the Journal.
e) that the Author abides by all other provisions of the Journal's Code of Ethics.
The Editor-in-Chief and the Executive Editors reserve the right not to publish contributions that do not comply with the editorial criteria. Authors only are exclusively responsible for the contents of their writings. Anonymous writings are not accepted.
All contributions are published in PDF format. Off-prints may be downloaded and printed.
Editorial criteria are available online, in the relevant section of the Journal.

Diritto e politica dei trasporti

Fascicolo 2/2024 anno 7, n. 13

Data Protection e *Data Retention*: la sicurezza nell'uso dei dati PNR*

Maria Pia d'Antuono

Dottoranda di ricerca in Scienze Giuridiche e Sociali per l'Innovazione presso l'Università degli Studi della Campania "Luigi Vanvitelli"

Abstract

Data Protection and Data Retention: security in the use of PNR data.

In recent years, the control over our lives has been fostered using technology, which, due to its intrusiveness, allows the monitoring of large flows of information that may contain numerous elements from which to infer habits, geolocation, and communication patterns. Faced with this new challenge, the supranational legislature first, and the national legislature later, has been active with regulatory interventions aimed at regulating the matter and meeting the delicate balance between the free movement of personal data and their necessary protection. Without claiming to be exhaustive, the following paper proposes an analysis on the necessary but considered balance between securitarian needs and those aimed at protecting individual freedoms in order to avoid that, in the name of security, the very fundamental principles on which democracy itself is based are compromised.

Negli ultimi anni, il controllo sulle nostre vite è stato favorito dall'utilizzo della tecnologia che, per la sua intrusività, permette di monitorare grandi flussi di informazioni che possono contenere numerosi elementi da cui desumere abitudini, geolocalizzazioni e modelli di comunicazione. Di fronte a questa nuova sfida, il legislatore sovranazionale prima, e quello nazionale poi, si sono attivati con interventi normativi volti a disciplinare la materia e a raggiungere il delicato equilibrio tra la libera circolazione dei dati personali e la loro necessaria protezione. Il saggio propone un'analisi sul necessario ma ponderato bilanciamento tra le esigenze securitarie e quelle di tutela delle libertà

* Sottoposto a referaggio.

individuali per evitare che, in nome della sicurezza, vengano compromessi i principi fondamentali su cui si basa la stessa democrazia.

Key words: General Data Protection Regulation, Passenger Name Record, Principle of proportionality, Balancing of rights, Data Retention.

Parole chiave: General Data Protection Regulation, Passenger Name Record, principio di proporzionalità, bilanciamento dei diritti, Data Retention.

Sommario – 1. Premessa – 2. Il *General Data Protection Regulation* GDPR – 3. Il *Passenger Name Record* PNR – 4. *Data Retention* e il riconoscimento biometrico alla luce del caso Ryanair – 5. Considerazioni conclusive: il rischio del Panopticon Digitale.

1. Premessa

Negli ultimi anni il controllo sulle nostre vite è stato potenziato dall'uso della tecnologia che, per la sua intrusività, consente il monitoraggio di grandi flussi di informazioni che possono contenere numerosi elementi da cui desumere abitudini, geolocalizzazioni e modalità di comunicazione.
Il processo di globalizzazione, l'evoluzione dei mezzi tecnologici, la sottile ma incisiva invadenza della rete internet e gli attuali problemi di sicurezza nazionale hanno evidenziato la necessità di implementare una protezione più efficace e innovativa nel trattamento dei dati personali rispetto al passato.[1] Di fronte a questa nuova sfida, il legislatore sovranazionale prima, e quello nazionale poi, non sono rimasti inerti, ma si sono attivati con diversi interventi normativi tesi a regolamentare la materia e a realizzare il delicato bilanciamento tra la libera circolazione dei dati personali e la loro necessaria protezione.[2]
Emerge, quindi, una nitida contrapposizione la necessità di soddisfare gli interessi specifici del titolare del trattamento e la protezione del soggetto coinvolto.

1. "L'avvento della società dell'informazione può essere infatti registrato come quel passaggio da un "prima", nel quale il principale problema di chi gestiva dati e informazioni era riuscire a diffonderli qualora volesse o dovesse dare ad essi pubblicità, a un "dopo", nel quale, invece, chi gestisce dati incontra difficoltà quando voglia impedire che "tutti sappiano tutto" indiscriminatamente", così D. MARONGIU, *I dati delle pubbliche amministrazioni come patrimonio economico nella società dell'informazione*, in *Informatica e diritto*, XVIII, 2008, n. 1-2, p. 355. Per ulteriori approfondimenti, si v. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973; G. ARENA, *La tutela della riservatezza nella società dell'informazione*, in AA.VV., *Scritti in onore di Pietro Virga*, I, Milano, 1994, p. 70 ss.
2. Il diritto ad essere lasciati soli è stato soppiantato dal diritto alla tutela dei dati personali, nonché strumento atto a contrastare una nuova forma di controllo più avanzata e pervasiva: il potere informatico. AA.VV., *La tutela della privacy informatica. Problemi e prospettive*, (a cura di V. FRANCESCHELLI), *Studi di diritto dell'economia*, Milano, Giuffrè, 1998.

La crescente mole di dati generati dal mondo digitale, unita all'evoluzione di tecnologie sempre più complesse e avanzate, ha reso la raccolta e il trattamento delle informazioni personali un processo sempre più pervasivo e, al contempo, difficile da monitorare.[3]
Uno dei settori in cui emergono tensioni significative tra la sicurezza, quale bene costituzionalmente protetto, e i diritti fondamentali è quello in cui la salvaguardia del diritto alla privacy può costituire un ostacolo per la protezione della sicurezza intesa sia come valore individuale che collettivo.[4]
Il presente contributo si propone di analizzare il complesso e intricato rapporto tra libertà individuale e sicurezza, con particolare attenzione alla tutela offerta dall'ordinamento eurounitario e italiano in materia di concorrenza e protezione dei dati personali. Sebbene tradizionalmente interpretate in un'ottica di contrapposizione, tali dimensioni richiedono oggi una rilettura che ne evidenzi la complementarità e l'interconnessione.[5]
La ricerca si pone l'obiettivo di dimostrare che il diritto alla protezione dei dati personali debba essere inteso come uno strumento al servizio dell'uomo, evitando di configurarlo come prerogativa assoluta, ma collocandolo nel contesto della sua funzione sociale e bilanciandolo con altri diritti fondamentali, nel rispetto del principio di proporzionalità.[6]

3. La portabilità dei dati è un principio chiave del Regolamento Generale sulla Protezione dei Dati dell'UE. Considerando l'ampia interpretazione del concetto di "dato personale", il diritto alla portabilità si estende ad una vasta gamma di dati, generando talvolta sovrapposizioni e conflitti con altri interessi. G. ETTORE, *Dati personali (tutela dei)*, in *Enc. diritto*, 1999. Tra i tanti, si v. V. FRANCESCHELLI, *Computer e diritto*, Rimini, Maggioli, Ed., 1989; G. ALPA, B. MARKESINIS, *Il diritto alla "privacy" nell'esperienza di "common law" e nell'esperienza italiana*, in *Riv. trim. dir. proc. civ.*, n. 2, 1997; G. ALPA, *La disciplina dei dati personali*, Roma, 1998; AA.VV., (a cura di V. FRANCESCHELLI) *La tutela della privacy informatica. Problemi e prospettive*, in *Studi di Diritto dell'Economia*, Milano, Giuffré, 1998; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006; F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Torino, Giappichelli, ed. 2016; G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessioni*, in *Contratto e impresa*, 2017, p. 723 ss.
4. Il crescente ricorso a nuove tecnologie di sorveglianza in funzione di attività investigativa è un fenomeno oramai diffuso, legato in gran parte al chiaro spostamento dell'attenzione nelle indagini penali dalla tradizionale sfera repressiva a quella preventiva. Cfr. F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, 2018, disponibile online. Per altri approfondimenti, si v. A. VEDASCHI, *Intelligenza artificiale e misure antiterrorismo alla prova del diritto costituzionale*, in *Consulta online*, 17 febbraio 2020, p. 2.
5. M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018, p. 82. Per approfondimenti, si v. L. CASINI, *Lo Stato ai tempi di Google*, Milano, 2020; R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA, *Codice della Privacy e data protection*, Milano, 2021.
6. Considerando 4 del Regolamento 2016/679/UE. G. FINOCCHIARO, (a cura di) *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; ID, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civ. comm.*, 2017, p. 1 ss.

2. Il *General Data Protection Regulation* GDPR

L'entrata in vigore del Regolamento UE n. 679 del 2016 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" ha abrogato e sostituito la Direttiva 95/46/CE, per anni pietra angolare della normativa dell'Unione Europea in materia di protezione dei dati personali.[7]
Rispetto al tentativo di armonizzazione avviato con la Direttiva 95/46/CE, l'attuazione del GDPR porta ad una normativa uniforme in tutti i paesi UE, caratterizzata da un insieme di regole comuni rispetto ai diritti degli interessati e agli obblighi di coloro che effettuano il trattamento dei dati; il provvedimento si distingue per l'obiettivo di assurgere a punto di riferimento per l'intera legislazione europea, riducendo, se non eliminando del tutto, la frammentazione e l'incertezza normativa che la Direttiva 95/46 non era riuscita ad evitare.[8]

7. Nel disposto di cui al Considerando 9, il legislatore europeo riconosce espressamente che la Direttiva 95/46/CE "non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione [...] che [...] le operazioni online comportino rischi per la protezione delle persone fisiche" in E. LUCCHINI GUASTALLA, Privacy e Data Protection: principi generali, in E. BATTELLI, *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019, p. 57. Con l'entrata in vigore del GDPR, la Direttiva 95/46/CE è stata definitivamente abrogata, così come le leggi nazionali sulla protezione dei dati adottate durante la sua applicazione (cfr. art. 94 GDPR). Tali normative nazionali restano efficaci e applicabili esclusivamente nei casi in cui il GDPR stesso prevede un rinvio al legislatore nazionale dei singoli Stati membri. Al di fuori di quest'ambito, le leggi nazionali che risultano in contrasto con la normativa europea devono essere disapplicate (cfr. art. 16 TFUE). Per altri approfondimenti, si v. E. CARLONI, *Le linee guida del garante: protezione dei dati e protezione dell'opacità*, in *Giornale Dir. Amm.*, 2014; M. CASTELLANETA, *L'incidenza del regolamento GDPR sul quadro normativo esistente*, in *Notariato*, 2018; E. FACCIOLI & M. CASSARO, *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi di accountability e privacy by design*, in *Dir. ind.*, 2018; F. TIGANO, *Protezione dei dati personali e pubblica amministrazione: alcuni spunti di riflessione*, in *Dir. soc.*, 2, 2022.

8. La differenza tra la Direttiva 95/46/CE e il Regolamento 2016/679 riflette l'evoluzione dell'ordinamento giuridico europeo, che ha altresì determinato un mutamento significativo della base di legittimità del secondo rispetto alla prima. La Direttiva 95/46/CE riconosceva la protezione dei dati personali come un diritto fondamentale e sottolineava la necessità di armonizzare le normative degli Stati membri per favorire la libera circolazione dei dati all'interno della Comunità Economica Europea. Il GDPR, invece, si distingue per la sua maggiore completezza normativa, basandosi sull'imperativo di garantire pienamente il diritto fondamentale alla protezione dei dati personali, come sancito dalla Carta dei Diritti Fondamentali e dal Trattato di Lisbona. Sul punto, si v. F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 8 ss. Si veda anche A. PALLOTTA, *Regolamento europeo n. 679/2016: profili di continuità e aspetti innovativi*, in *Mercato unico digitale, dati personali e diritti fondamentali*, in *Rivista Eurojus*, luglio 2020, p. 95. "Le ricadute normative del Regolamento, per quanto riguarda la situazione italiana, sono compendiate nel d.lgs. 10 agosto 2018, n. 101 contenente "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016", che ha armonizzato ed integrato il d.lgs. 30 giugno 2003, n. 196, Codice privacy al GDPR, ed il cui iter di validazione è stato piuttosto travagliato" così F. BRIZZI, *Privacy; la tutela penale dei dati personali*, Giuffré, 2020, p. 4.

In questo contesto, il GDPR ha rappresentato un'occasione cruciale non solo per stabilire un livello di regolazione della protezione dei dati personali capace di ridurre le divergenze tra i vari ordinamenti nazionali, ma anche per assicurare un bilanciamento tra la tutela dei dati e la loro circolazione nel mercato interno.[9]

Il Regolamento ha introdotto una serie di novità che riguardano sia la tutela dei soggetti interessati, o comunque della parte vulnerabile del trattamento, sia, in modo più specifico, il titolare, inteso come la persona fisica che esercita un'attività di trattamento del dato indipendentemente dalla natura economica della sua attività.[10] Per certi versi, sembra che il Regolamento ribalti la prospettiva della Direttiva, concentrandosi maggiormente sui diritti, sugli obblighi e sulle misure di sicurezza che riguardano il Titolare e il Responsabile, piuttosto che sui diritti dei *data subject*: la protezione dei dati, che in precedenza veniva affrontata dal punto di vista dei diritti degli interessati, appare ora considerata principalmente dall'altro punto di vista.

In generale, si evince chiaramente quanto il *leitmotiv* del GDPR faccia ben intendere come la sua disciplina sia destinata a tutelare le persone fisiche indipendentemente dalla loro nazionalità o residenza, in relazione al trattamento dei loro dati personali.

Una volta entrati nello spazio virtuale di internet, gli individui sembrano proiettati in una dimensione giuridica parallela, dominata da soggetti capaci di controllare le vite dei singoli ben oltre le tradizionali prerogative degli Stati nazionali. Il GDPR, con la sua articolata regolamentazione, riflette il timore che gli individui possano ridursi a semplici dati, mentre grandi multinazionali,

9. Sul bilanciamento dei diritti nel quadro europeo della protezione dei dati, tra i tanti si v. F. PIZZETTI *Op. loc. cit.*, p. 225 ss; N. ZORZI GALGANO, L*e due anime del GDPR e la tutela del diritto alla privacy*, in *Persona e Mercato dei dati. Riflessioni sul GDPR*, 2019, p. 35 ss.

10. Per ulteriori approfondimenti, si v. F. PIZZETTI, *Op. loc. cit.*, p. 153 ss. L'art. 4 del Regolamento UE 2016/679, Fornisce le fondamentali definizioni di "trattamento" e di "dato personale". Per "trattamento" s'intende "Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". In combinato disposto, è utile richiamare la lettura dell'art. 9 del Regolamento UE 2016/679, secondo cui "titolare del trattamento" si intende "La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri". Per ulteriori approfondimenti, si v. R. MONTINARO, *Tutela della riservatezza e risarcimento del danno nel nuovo "Codice in materia di protezione dei dati personali"*, in *Giust. civ.*, n. 5, 2004; S. CALZOLAIO, P*rotezione dei dati personali, estratto da Digesto delle Discipline Pubblicistiche*, Utet, 2017, p. 627; G. ALPA, G. RESTA, *Le persone e la famiglia*, in *Le persone fisiche e i diritti della personalità*, Torino, 2020; A. SANDULLI, *Lo "Stato digitale". Pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in *Riv. trim. dir. pubbl.*, n.2, 2021, p. 513 ss.

grazie alla capacità di raccogliere enormi quantità di informazioni tramite complessi algoritmi, consolidino posizioni dominanti e poteri di mercato straordinari in questa realtà virtuale.[11]
La formulazione contenuta nel Considerando 7 GDPR, secondo cui "è opportuno che le persone fisiche abbiano il controllo dei dati che li riguardano", rappresenta un passaggio fondamentale che introduce una significativa innovazione rispetto all'impostazione tradizionale. Tale approccio, consolidatosi prima con la Convenzione del 1981 e poi con la Direttiva 95/46, ancorava la tutela dei dati personali principalmente alla tutela della dignità e dell'identità della persona.[12] La nuova prospettiva si distingue per la capacità di offrire una visione più equilibrata, che integra la protezione dei dati personali con l'esigenza di incentivare il libero flusso delle informazioni nell'ambito dell'economia digitale, ampliandone ulteriormente la portata.[13]
Quanto testé evidenziato mette in luce una connessione continua con la Direttiva 95/46/CE attraverso principi già esistenti: il fine perseguito dal legislatore europeo è stato quello di adeguare l'apparato legislativo alle nuove esigenze di protezione degli interessati e al progresso nel nuovo ambiente digitale, perseguendo l'obiettivo europeo di instaurare quel clima di fiducia e di certezza giuridica necessario per lo sviluppo (anche) dell'economia digitale in tutto il mercato interno.[14]
Il fatto che i dati debbano essere trattati in modo da non compromettere le libertà e i diritti delle persone evidenzia l'importanza del principio di correttezza, che si affianca alla liceità e alla trasparenza e che, ove applicato specificamente nei rapporti tra il titolare del trattamento e l'interessato, assume

11. N. BRUTTI, *Le figure soggettive delineate maiuscolo dal GDPR: la novità del data Protection officer*, in V. FRANCESCHELLI, E. TOSI, (a cura di) *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e Nuovo Codice Privacy*, 2019, p. 120; B. PONTI, *Il luogo adatto dove bilanciare. Il posizionamento del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in *Le istituzioni del federalismo*, 2019, p. 525 ss.
12. Si tratta del cd. principio dell'autodeterminazione informatica di matrice tedesca secondo cui ogni individuo è titolare del diritto di determinare autonomamente le modalità di divulgazione e di utilizzo dei propri dati personali. F. LAVIOLA, *Il diritto all'autodeterminazione informativa tra concorrenza e data protection. Riflessioni a margine della saga Facebook c. Bundekartellamt nella giurisprudenza delle corti tedesche e in attesa della Corte di Giustizia*, in E. CREMONA, F. LAVIOLA e V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.
13. F. PIZZETTI, *Op. loc. cit.*, p. 14 ss. Il Regolamento deve essere letto e applicato avendo chiaro che i trattamenti dei dati personali devono essere effettuati garantendo un equilibrio tra due obiettivi di pari rilevanza: da un lato è fondamentale tutelare il diritto alla protezione dei dati personali, evitando di compromettere la libertà e i diritti della persona; dall'altro, è necessario assicurare la più ampia libertà di circolazione dei dati all'interno del quadro Europeo. Per altri approfondimenti, si v. ID, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 166.
14. Cons. 5-6-7 GDPR. Il nuovo Regolamento non solo si pone l'obiettivo di tutelare i dati delle persone fisiche, ma anche quello di "dare un quadro più solido e coerente in materia di protezione dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare un clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno" (Cons. 7 GDPR). Già la Direttiva 95/46, all'articolo 1, stabiliva un divieto specifico per gli Stati di restringere o limitare la circolazione dei dati per ragioni legate alla tutela dei dati personali (Considerando 3 GDPR).

una nuova colorazione, garantendo sia un'interazione leale dei diritti e delle aspettative degli individui coinvolti, sia un rispetto delle esigenze di tutela dell'interessato nella prospettiva di un bilanciamento proporzionale che spesso è rimesso al titolare del trattamento.[15] La responsabilità del titolare non si esaurisce, infatti, nella sola valutazione e adozione di misure di sicurezza adeguate, ma richiede altresì un costante monitoraggio e una conseguente documentazione delle attività svolte, rafforzando quell'operazione di "rendicontazione" intesa sia come accessibilità alle informazioni da parte dell'interessato, sia come garanzia alle attività svolte dall'operatore nel rispetto della normativa di settore.[16]

In questo senso, un'ulteriore norma cardine del Regolamento è l'art.5, par. 1, lett. *f*, che stabilisce che i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza (dei dati personali), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale". Invero, anche il principio di sicurezza pone in evidenza l'importanza di una valutazione costante e attenta ai rischi connessi al trattamento dei dati, consentendo di apprezzare la relazione di responsabilità che intercorre tra il titolare e il responsabile del trattamento: entrambi sono chiamati non solo a garantire la conformità alle norme ma anche a svolgere un ruolo attivo nella protezione dei dati, adottando misure tecniche e organizzative adeguate e continuamente aggiornate.[17]

Nel GDPR cambia la concezione della sicurezza che assume una portata più ampia rispetto a quanto previsto dalla Direttiva 95/45: non è più considerata un aspetto separato, legato esclusivamente agli obblighi dei titolari e demandato alla regolazione degli Stati membri, ma diviene elemento essenziale dei trattamenti che dovranno garantire un'adeguata protezione dei dati, includendo provvedimenti volti a prevenire trattamenti illeciti o non autorizzati, nonché la perdita, la distruzione o il danneggiamento accidentale dei dati.

La protezione dei dati personali conosce dunque un significativo rafforzamento con l'innesto della sicurezza quale principio cardine;[18] l'implementazione di meccanismi di controllo del rischio sin dalle fasi iniziali del trattamento, unitamente all'obbligo di monitoraggio e reazione continua,

15. Artt. 5-11 GDPR. F. BRAVO, *Il principio di solidarietà tra Data protecion e Data governance*, in Diritto dell'Informazione e dell'Informatica (Il), 3, 1giugno 2023, p. 481. Cfr. Considerando n. 4 GDPR.

16. Cfr. art. 24, co.3, Regolamento UE 2016/679, S. CALZOLAIO, Op. cit., p. 631. Per ulteriori approfondimenti, si v. E. FACCIOLI, M. CASSARO, *Il "GDPR"e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *dir. industriale*, VI, 2018; A. ALONGI & F. POMPEI, *Diritto della privacy e protezione dei dati personali: il GDPR alla prova della data driven economy*, Casalini, 2021.

17. Alla luce degli obblighi imposti al titolare del trattamento, in particolare quelli previsti dagli artt. 24 e 32 GDPR, emerge chiaramente l'affermazione di un approccio regolatorio responsabilizzante. Cfr. M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Responsabilità Civile e Previdenza*, 4, 1° aprile 2020, p. 1343. I principi stabiliti nel Regolamento sono interconnessi con una serie di obblighi a carico dei titolari del trattamento e con una serie di diritti spettanti ai soggetti cui i dati personali si riferiscono. Sul punto si v. L. TORCHIA, *Lo Stato digitale. Una introduzione*, in il Mulino, 2023, p. 56 ss.

18. Cfr. Artt. 33-34 GDPR.

evidenzia come la sicurezza sia un valore intrinseco al trattamento che si impone come principio centrale e direttamente efficace nei rapporti tra titolare, responsabile e soggetti interessati.[19]
In questa prospettiva, garantire la sicurezza nel cyberspazio si rivela imprescindibile per tutelare il pieno esercizio dei diritti fondamentali in un contesto digitale che non rappresenta più una nicchia riservata ad attività specifiche, ma abbraccia l'intera collettività, incidendo sulla quotidianità della vita sociale e professionale.[20]
Secondo il disposto normativo di cui all'art. 33, co. 1, GDPR "in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".
La configurazione di un obbligo generale di notifica da parte del titolare del trattamento per ogni violazione costituisce la concretizzazione del principio di *accountability* che emerge come principio immanente e criterio generale di attribuzione della responsabilità.[21]
Si tratta di un dovere fondato sulla procedimentalizzazione della gestione del rischio, calibrato in relazione alla natura e alla gravità della violazione dei dati personali, nonché alle tipologie di rischio cui possono essere esposte le persone fisiche coinvolte.[22]

19. M. RENNA, *Op. loc. cit.*
20. Per altri approfondimenti, si v. A. BALDASSARRE, voce *Libertà. 1) Problemi Generali*, in *Enc. Giur.*, XIX, Roma, 1990; T.GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, in *Forum di Quaderni Costituzionali*, 2008; M. DOGLIANI, *Il volto costituzionale della sicurezza*, in G.COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012, p. 1; A.SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal –Rivista di BioDiritto*, n. 1, 2019; G.DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, 2019; S. ROSSA, *Cybersicurezza e pubblica amministrazione*, Napoli, 2023; G. ZICCARDI, *Dati Avvelenati*, Milano, Raffaello Cortina Editore, 2024; L. MORONI, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi*, 14, 2024, p. 180.
21. Più specificatamente si potrebbe collocare in una situazione intermedia, a metà strada tra responsabilità e compliance, poiché il titolare è tenuto a rispettare la normativa in esame (*compliant*). A. PALLOTTA, *Op. loc. cit.* "La *ratio* sottesa al principio di *accountability* sembra essere proprio quella di favorire il passaggio dalla teoria dei principi alla loro messa in pratica, traducendo gli obblighi giuridici in misure verificabili nei fatti e non solo su carta.". Si v. anche R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Ciberspazio e diritto*, 19, 2018, p. 213.
22. M. RENNA, *Op. loc. cit.* Tra le diverse disposizioni che contemplano il nuovo principio di accountability, la principale è l'art. 24 che affida alla discrezionalità del titolare del trattamento la decisione delle misure da adottare: discrezionalità libera ma non illimitata, anzi necessariamente parametrata alle condizioni indicate nello stesso disposto normativo di cui all'art. 24 GDPR. E così, l'art. 7 GDPR rimette al titolare la scelta della modalità di acquisizione del consenso al trattamento e del conseguente onere della prova e l'art. 12 GDPR assegna al titolare la scelta delle misure appropriate per fornire all'interessato le informazioni richieste. Sul punto, si v. R. CARLEO, *Il Principio di Accountability nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo diritto civile*, anno VI, n. 1, 2021, p. 368.

Pur potendo apparire un'estensione del principio di trasparenza, il principio di *accountability* va oltre la semplice garanzia di accesso dell'interessato alle informazioni sulle attività di un dato operatore, richiedendo che il titolare del trattamento sia in grado dimostrare la conformità di tali attività alla normativa vigente.[23]

Il dettato normativo dell'articolo 12 riveste particolare importanza poiché, in linea con una concezione innovativa della protezione dei dati personali, colloca l'interessato al centro del sistema, attribuendogli un ruolo primario rispetto alla stessa tutela giuridica.

Il principio di trasparenza in esso contenuto si estende all'obbligo, in capo al titolare del trattamento, di adottare tutte le misure appropriate per fornire all'interessato l'informativa necessaria per comprendere il contenuto e le modalità di esercizio dei diritti previsti dallo stesso Regolamento, tra questi il diritto alla cancellazione.

A tal riguardo, sin dal Preambolo del Regolamento, si riconosce all'interessato il diritto di ottenere la rettifica dei dati che lo riguardano e il diritto alla cancellazione, qualora la conservazione di tali dati violi le disposizioni europee. In particolare, l'interessato può richiedere la cancellazione e l'interruzione del trattamento dei propri dati quando questi non siano più necessari per le finalità per cui sono stati raccolti (Considerando 65). In aggiunta, il Considerando 66 rafforza il diritto all'oblio nel contesto digitalizzato, prevedendo che il titolare del trattamento debba altresì informare gli altri soggetti che trattano gli stessi dati dell'obbligo di cancellare qualsiasi link, copia o riproduzione dei dati stessi.[24]

In questa prospettiva si colloca il comma 2 dell'art. 17 del GDPR, che, tra la mera richiesta di cancellazione tempestiva dei dati personali da parte dell'interessato (comma 1) e l'esigenza di bilanciare il diritto alla cancellazione con la tutela della libertà di espressione (comma 3), introduce

23. A riguardo, cfr. art. 24 del GDPR sull'adesione del titolare del trattamento ad un codice di condotta (art. 40 e 43 GDPR).

24. P. SAMMARCO, *Privacy Digitale*, in V. FRANCESCHELLI, E. TOSI, *Op. cit.*, p. 168. Giova evidenziare che la prima formulazione del diritto all'oblio riguardava il contesto *offline* e consisteva nel diritto di una persona a non subire danni derivanti dalla ripubblicazione non necessaria di una notizia risalente nel tempo, originariamente divulgata in modo lecito. Per ulteriori approfondimenti si v. Cass. Civ. Sez. III, 9 Aprile 1998, n. 3679, in Foro.it, I, 1998, p. 834; A seguito della celebre decisione della Corte di giustizia del 13 maggio 2024 nel caso Google Spain, si è acceso un ampio dibattito sul riconoscimento di un diritto all'oblio di portata generale che, con l'entrata in vigore del GDPR, ha trovato una specifica disciplina normativa, consolidando il suo *status* giuridico. La riflessione sul diritto all'oblio si è sviluppata a partire dagli anni 60 del XX secolo come naturale evoluzione del concetto di privacy, inteso come "right to be let alone", e si radica nel riconoscimento della solitudine come presupposto per l'esercizio della libertà individuale, evidenziando l'esigenza di tutelare l'individuo non solo dalla diffusione illecita di informazioni personali, ma anche dal perpetuarsi di informazioni obsolete e pregiudizievoli nel tempo, in linea con l'evoluzione del diritto alla riservatezza. S. D. WARREN, L. S. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, Boston, 1890. L'opera rappresenta una pietra miliare in materia di privacy; si tratta della prima monografia giuridica a riconoscere l'esistenza di un autonomo diritto alla privacy. Prima di allora, non solo non si comprendeva la natura giuridica e quella degli elementi che complessivamente costituivano il diritto alla riservatezza, ma neppure si riusciva ad individuare quale fosse il principio ispiratore o diritto fondamentale che lo legittimasse.

una significativa innovazione imponendo un nuovo obbligo al titolare del trattamento.[25] Nello specifico, qualora i dati personali siano stati resi pubblici e debbano essere cancellati ai sensi del comma 1, il titolare del trattamento è obbligato a adottare misure ragionevoli, comprese soluzioni tecniche, per informare gli altri titolari del trattamento della richiesta dell'interessato di rimuovere qualsiasi link, copia o riproduzione dei dati personali, tenendo conto della tecnologia disponibile e dei costi di attuazione.[26]

Oltre ai diritti appena esaminati, merita particolare attenzione il diritto alla portabilità dei dati, che rappresenta una significativa evoluzione nell'ambito dei trattamenti automatizzati.[27]

L'intermediazione delle piattaforme digitali nelle transazioni commerciali ha comportato, da un lato, un grado di dipendenza delle imprese dalle piattaforme online in costante aumento e, dall'altro, ha costretto i consumatori ad utilizzarle come mezzo principale per accedere a offerte di beni e servizi. Questo modello di funzionamento, tipico dei mercati digitali, ha sollevato una serie di questioni non di poco rilievo. Tra queste, oltre alla tutela della concorrenza, spicca la protezione dei dati personali, divenuti indispensabili per le imprese nell'analisi delle tendenze di mercato.[28]

25. Ad una prima analisi, l'articolo in questione, in specie nei commi 1 e 3, non sembra offrire il livello di innovazione che forse ci si sarebbe potuti aspettare. Tuttavia, le disposizioni introdotte evidenziano un richiamo alla precedente disciplina della cancellazione (articolo 12 della direttiva 45/96/CE). Si v. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. RESTA, V. ZENO ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spai*n, Roma, 2015, p. 596. Tra i più che si sono occupati del diritto all'oblio, si v. D. MESSINA, *Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione*, in *Informat. dir.*, 2009; D. MINIUSSI, *Il "diritto all'oblio": i paradossi del "caso Google"*, in *Riv. it. dir. pubbl. com*, 2015; A. VIGLIANISI FERRARO, *La sentenza Google Spain ed il diritto all'oblio nello spazio giuridico europeo*, in *Contr. impr. Eur.*, 2015; M. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, in *Dir. fam. pers.*, 2015; D. BARBIERATO, *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento UE 2016/679 sulla protezione dei dati personali*, in *Responsabilità Civile e Previdenza*, 6, 1° giugno 2017, p. 2100; F. DI CIOMMO, Il diritto all'oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali, in Foro.it, V 6, 9, 2017; A.L. VALVO, I*l diritto all'oblio nell'epoca dell'informazione "digitale"*, in *St. integr. eur.*, 2015; S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in *Federalismi*, 15, 2018.

26. Giova però evidenziare che la norma non impone al titolare, a cui l'interessato ha indirizzato la richiesta di cancellazione, l'onere di verificare se anche gli altri titolari abbiano adempiuto alla richiesta e di informare conseguentemente l'interessato. Ciò è comprensibile per evitare di gravare ulteriormente il titolare con un onere eccessivo.

27. Già riconosciuto in altri ambiti come quello della telefonia con riferimento alla portabilità del numero telefonico.

28. C. COLAPIETRO, *Il diritto alla portabilità dei dati e l'evoluzione del quadro normativo*, in *Diritti Fondamentali*, 2, 2023, p. 3 ss. Il tema della portabilità dei dati rappresenta un aspetto cruciale nell'ambito della protezione dei dati personali. Prima ancora di essere introdotto nel GDPR, il concetto di portabilità ha iniziato a prendere piede all'interno del mondo imprenditoriale, mostrando come le aziende digitali avessero già intuito l'importanza di garantire agli utenti un maggiore controllo sui propri dati. F. CATALANO, *Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale*, in *Europa e diritto privato*, 3, 2019, p. 833-865; Sul tema si v. tra i più F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le Nuove Leggi Civili Commentate*, 2, 2017, p. 372-372; R. CAVALLO PERIN, *Ragionando come se l'amministrazione*

In tale contesto si inserisce il concetto di portabilità, sancito dall'articolo 20 del GDPR, che, nella nuova prospettiva, acquisisce un ruolo fondamentale. Da un lato evidenzia l'importanza strategica dei dati e delle informazioni per chi opera nel settore del business; dall'altro offre ai soggetti interessati un maggiore controllo sui propri dati, rafforzandone la posizione.[29]
Il diritto alla portabilità può essere definito come la facoltà di trasferire integralmente, senza vincoli, insiemi di informazioni, acquisendole personalmente o facendole circolare direttamente tra i titolari.
Nonostante opinioni divergenti circa la sua portata applicativa il diritto alla portabilità dei dati si realizza nella possibilità, per l'interessato, di ottenere i propri dati in un formato strutturato, di uso comune e leggibile da dispositivi elettronici automatici, nonché nella possibilità di trasferirli, direttamente o tramite terzi, a un nuovo titolare del trattamento, senza che il titolare originario che li ha forniti possa frapporre ostacoli.[30]
Emerge chiaramente la prospettiva di convergenza tra le diverse discipline: il diritto alla portabilità si propone di potenziare il controllo degli interessati sui propri dati e, al contempo, di favorirne la circolazione, incentivando così la concorrenza tra titolari all'interno dell'Unione Europea.

3. Il *Passenger Name Record* PNR

La disciplina europea in materia di protezione dei dati personali si caratterizza per un'impostazione articolata e complessa. Un ruolo fondamentale è ricoperto da strumenti normativi complementari, concepiti per rafforzare le garanzie individuali e assicurare una regolamentazione coerente tra gli Stati Membri.

fosse data, in *Dir. Amm.* 2, 2020, p. 305 ss; M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il reno)*, in *Dir. informazione e informatica*, 2, 2021.

29. Cfr. Il diritto di accesso nel fornire all'interessato la copia dei dati oggetto del trattamento. Il forte legame tra il diritto alla portabilità e quello di accesso è dimostrato altresì dall'origine del primo che, originariamente, era stato proposto nell'ambito dello stesso diritto di accesso, formando così da un unico diritto di accesso e ottenimento dei dati. Diversamente dal diritto di accesso, il diritto alla portabilità è subordinato a particolari condizioni di operatività (si v. art. 20, paragrafo 1). Per altri approfondimenti, si v. E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati*, in E. TOSI (a cura di) *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy*, Giuffrè, 2019, p. 189-202.

30. Alcuni hanno evidenziato la sussistenza di rischi per la riservatezza. Sul punto, si v. E. BATTELLI, G. D'IPPOLITO, *Op. loc. cit.*; Per un approfondimento, si v. S. FAMILIARI, *Il diritto alla portabilità dei dati: origine e prospettive per il futuro*, in *Ciberspazio e diritto*, 17, 56 3-2016, p. 403-435; S. BARTH, M.D.T. DE JONG, *The privacy paradox, Investigating discrepancies between expressed privacy concerns and actual online behavior, A systematic literature review*, in *Telematics and Informatics*, n. 34, p. 2017; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi*, 2018; G. PALMA, *La portata fortemente innovativa del diritto alla portabilità dei dati come articolato nel GDPR e nelle linee guida WP29*, in *Riv. giur. Data Protection Law*, n. 2, 2019, p. 50 ss.; J. BAZZOLI, *La portabilità dei dati personali*, in *Ciberspazio e diritto*, vol. 20, n. 62 1-2 – 2019, p. 133-160.

In tale ottica si collocano le Direttive UE 680/2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali, e 681/2016 sull'utilizzo dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale in relazione a reati di terrorismo e reati gravi.
Questi strumenti, insieme al Regolamento (UE) 679/2016, sono parte di un unico pacchetto di riforma adottato dall'Unione Europea per potenziare la protezione dei dati. Sebbene mirino a potenziare le garanzie per gli interessati, le direttive attengono più specificamente al trattamento delle informazioni personali nell'ambito delle attività investigative e di perseguimento dei reati, con particolare riferimento alla cooperazione transfrontaliera e all'armonizzazione normativa tra Stati membri.[31]
La Direttiva 680/2016 è speculare al Regolamento nel suo ambito di applicazione; molte delle norme in essa contenute sono simili a quelle presenti nel testo del GDPR, ma specifiche per il trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. L'obiettivo del provvedimento europeo in questione è agevolare l'utilizzo e il trasferimento di informazioni, rafforzando la cooperazione giudiziaria in materia penale e di polizia, al fine di rendere più efficaci la prevenzione e gli strumenti di contrasto alla criminalità e al terrorismo.
La Direttiva 681/2016, invece, si occupa del trattamento dei dati del cosiddetto *Passenger Name Record*, o Codice di prenotazione, contenente le informazioni relative al viaggio aereo di ciascun passeggero ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati di simile gravità.
Nonostante entrambe siano orientate all'azione penale e all'attività investigativa finalizzata alla prevenzione e alla repressione dei reati, le due direttive presentano differenze sostanziali in relazione ai soggetti coinvolti nella raccolta e nel trattamento dei dati. In particolare, secondo quanto disposto dalla Direttiva 680/2016, il trattamento può essere condotto esclusivamente da un'Autorità pubblica competente nei settori oggetto del trattamento o da entità delegate dallo Stato e da pubblici poteri; al contrario, nel contesto della Direttiva 681/2016, i soggetti coinvolti nel trattamento non sono limitati alle sole Autorità pubbliche, ma includono anche i vettori aerei che forniscono le informazioni dei passeggeri PNR.[32]

31. Una scelta ponderata quella del legislatore europeo che ha deciso di intervenire attraverso una serie di strumenti interconnessi, cercando di conciliare normative che rappresentassero un compromesso tra il potenziamento della protezione dei dati personali e la necessità di assicurare un livello adeguato di sicurezza collettiva nella prevenzione di atti terroristici. Si v. F. ROSSI DAL POZZO, *Protezione dei Dati personali e diritti fondamentali della persona: le nuove norme sui codici di prenotazione*, in *Riv. Dir. intern. priv. proc.*, 2016, p. 1020.
32. I dati PNR sono informazioni fornite dai passeggeri al momento della prenotazione del volo, del check – in e/o di imbarco; essi possono variare da compagnia a compagnia ed includono una serie di dettagli relativi al viaggio e l'identità di ciascun passeggero. Cfr. Allegato 1 Direttiva. I dati PNR sono ben più rilevanti rispetto ai dati API

Come è noto, il punto di svolta si è avuto con gli episodi dell'11 settembre del 2001, che non solo hanno segnato un momento cruciale nel bilanciamento tra libertà e sicurezza, ma hanno fatto emergere, su scala globale, anche la necessità di monitorare i dati di passeggeri ed equipaggi coinvolti nei trasporti aerei.[33]

La procedura legislativa relativa alla proposta di direttiva sui dati PNR ha avuto inizio il 6 novembre del 2007, quando la Commissione ha adottato una proposta di decisione quadro del Consiglio sull'uso dei dati del Codice di prenotazione nelle attività di contrasto al terrorismo e alla criminalità organizzata. Tuttavia, con l'entrata in vigore del TFUE, la Proposta del 2007, che non era stata adottata dal Consiglio, era divenuta obsoleta.

Di conseguenza, nel febbraio del 2011 la Commissione ha presentato un nuovo testo in cui ha individuato regole comuni per l'istituzione negli Stati membri di sistemi nazionali PNR, prevedendo che le compagnie trasferissero ad un'Autorità dedicata nello Stato membro di arrivo o di partenza, i dati relativi ai passeggeri dei voli internazionali disponibili nei rispettivi sistemi di prenotazione.[34]

La Proposta in parola è stata però respinta dalla Commissione Libertà civili, Giustizia e Affari interni del Parlamento europeo, che ne ha contestato la necessità e la proporzionalità.[35]

Advance Passenger Information che sono limitati all'insieme delle informazioni anagrafiche contenute nei documenti di identità acquisibili attraverso gli strumenti di lettura ottica o magnetica degli stessi.

33. Gli USA avevano dunque adottato una normativa che obbligava le compagnie aeree che operavano collegamenti con destinazione o partenza nel territorio degli Stati Uniti a fornire alle autorità doganali degli stessi Stati Uniti un accesso elettronico ai PNR. Dal canto suo, la Commissione Europea, ritenendo che tali disposizioni rischiassero di entrare in contrasto con la legislazione europea e con quella degli Stati membri in materia di tutela dei dati personali, avviarono dei negoziati con le autorità americane. Per ulteriori approfondimenti, si v. N. ROMANA, *Passenger Name Record PNR*, estratto da *Riv. dir. della navigazione*, n. 1, 2018, p. 187 ss.
34. Proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, doc. COM (2011) 32 def., 2011/0023 (COD) C7-0039/11 del 2 febbraio 2011. F. DI MATTEO, *La raccolta indiscriminata e generalizzata i dati personali: un vizio congenito nella direttiva PNR?*, in *Diritti umani e diritto internazionale*, in Il Mulino, n. 1, 2017, p. 216. Giova altresì aggiungere, già la disposizione di cui all'art. 3 della Proposta del 2011 prevedeva la creazione da parte degli Stati membri di un apposito ente preposto al trattamento dei dati PNR Unità di Informazione sui Passeggeri – UIP). Per ulteriori approfondimenti, si v. G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2, 2018.
35. Cfr. Garante europeo per la protezione dei dati, Doc. 2011/C/181/02 del 25 marzo 2011, in G.U.U.E. C184 del 22 giugno 2011. In particolare, si v. "P.8. La dimostrazione della necessità e della proporzionalità del trattamento dei dati è un presupposto indispensabile per l'istituzione del sistema PNR. Il GEPD ha già insistito in precedenti occasioni, segnatamente nel contesto di una possibile revisione della direttiva 2006/24/Ce (la «direttiva sulla conservazione dei dati») sul fatto che la necessità di trattare o conservare ingenti quantità di informazioni si dovesse basare su una chiara dimostrazione del rapporto tra uso e risultato, e dovesse consentire la valutazione sine qua non del fatto che risultati paragonabili si potessero ottenere con mezzi alternativi e meno invasivi della *privacy*."

A seguito degli attacchi terroristici di Parigi e della preoccupazione generale relativa alle minacce alla sicurezza interna dell'Unione Europea, la proposta di direttiva ha progressivamente riacquistato consensi.
Questo processo ha portato a un rafforzamento progressivo delle misure preventive, culminato con l'adozione della Direttiva 681/2016 del Parlamento europeo e del Consiglio, un testo che rappresenta un compromesso finalizzato all'armonizzazione dei diversi regimi nazionali in materia di trattamento dei dati per la prevenzione e il contrasto di reati gravi.[36]
Eppure, l'entrata in vigore della Novella ha destato non poche perplessità, evidenziando il rischio che potesse trasformarsi in uno strumento di raccolta indiscriminata di dati personali, contrapponendosi al quadro europeo.
In questo scenario, ogni individuo, per il solo fatto di spostarsi con un aeromobile al di fuori dei confini dell'Unione Europea, rischia di essere considerato un potenziale sospetto autore di reato, generando così presunzione di pericolosità, almeno fino a quando l'attività di profilazione sui dati raccolti non dimostri il contrario.[37]

4. *Data Retention* e il riconoscimento biometrico alla luce del caso Ryanair

Il crescente utilizzo della tecnologia nello svolgimento di pubblici servizi e funzioni, come quelle di investigazione e sorveglianza, ha reso particolarmente evidente l'urgenza di nuove regole per prevenire e correggere i rischi di violazione delle libertà personali e di discriminazione.
I vantaggi che questi strumenti offrono alle autorità investigative sono notevoli: dall'accuratezza delle analisi e alla rapidità dei risultati elaborati, fino alla versatilità di impiego di tali tecnologie.
Tuttavia, è opportuno evidenziare che, se la possibilità di raccogliere e archiviare una vasta quantità di dati personali offre indubbi vantaggi, essa presenta anche un potenziale altamente invasivo per la sfera privata, esercitando un impatto significativo sulla riservatezza individuale e generando una chiara tensione rispetto al diritto alla privacy, oltre a una sensazione di continua sorveglianza.[38]

36. Direttiva 2016/681/Ue del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, in G.U.U.E. L 119 del 4 maggio 2016. Per altri approfondimenti, si v. G. TIBERI, *La direttiva UE sull'uso dei dati del codice di prenotazione PNR nella lotta al terrorismo e ai reati gravi*, in *Quaderni Costituzionali*, n. 3, 2016, p. 591; Per altri approfondimenti, si v. anche S. SCAGLIARINI, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta* OnLine, n. 2, 2021, p. 489 ss.
37. Cfr. Principio di limitazione della conservazione (art. 5, co. 1, lett. e, GDPR); Base giuridica del Trattamento e Finalità (Art. 6 GDPR); Minimizzazione dei Dati (Art. 5, co.1, lett. c, GDPR); Proporzionalità e diritti fondamentali. Per altri approfondimenti si v. C. Giust. Ue, parere n. 1/15 del 26 luglio 2017. Sul punto, si v. N. ROMANA, *Passenger Name Record PNR*, estratto da *Riv. dir. della navigazione*, n. 1, 2018.
38. Si v. G. TODARO, *L'evoluzione delle fonti del diritto nella "società algoritmica": data retention e diritti fondamentali della persona – The evolution of the system of sources of law in the "algorithmic society": data retention and fundamental personal rights*, in *Cassazione Penale*, 1° giugno 2024, 6, p. 2011; O. POLLICINO, voce *Potere digitale*,

In questo contesto si inserisce il concetto di *data retention* che impone ai fornitori di servizi l'obbligo di conservare i dati per un periodo di tempo definito, consentendone l'acquisizione e l'accesso da parte delle pubbliche autorità per finalità di prevenzione e contrasto della criminalità.[39] In tal senso, la memorizzazione dei dati si configura come uno strumento imprescindibile per agevolare l'attività investigativa degli inquirenti che, parallelamente, si intreccia con i principi di rango costituzionale, richiedendo un delicato bilanciamento tra l'esigenza processuale di ricerca della prova e la salvaguardia dei diritti fondamentali della persona, rispettoso del principio di proporzionalità.[40]

Sebbene negli ultimi anni siano state introdotte normative volte a legittimare quella che viene definita sorveglianza di massa, ovvero un controllo preventivo esteso a tutti gli individui, indipendentemente dalla presenza di prove, indizi o sospetti di coinvolgimento in attività terroristiche, la necessità di verificarne la compatibilità con la tutela delle libertà individuali costituisce una sfida cruciale per le democrazie contemporanee e un tema sempre più frequentemente portato all'attenzione delle Corti, sia a livello nazionale e sovranazionale.[41]

in *Enc. Dir., I tematici*, V, Milano, 2023, p. 410 ss. Sulla "protezione spaziale della persona", si v. A. CAPONE, *Intercettazioni e Costituzione. Problemi vecchi e nuovi. Wiretapping and Constitution. Old and New Issue*s, in *Cassazione Penale*, 3, 2017, p. 1263; S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. spunti di diritto comparato*, in *Diritto dell'Informazione e dell'Informatica* (Il), 4, 1agosto 2023, p. 789; M. RAMAJOLI, *La convivenza tra trasparenza e riservatezza*, in *Diritto amministrativo*, 2, 1° giugno 2024, p. 471.

39. Tema al centro di un intenso dibattito legislativo, giurisprudenziale e dottrinario. Cfr. Direttiva 2006/24/CE e Direttiva 2002/58/CE. Sul punto, si v. A. CARDONE, *Il sistema del Data Retention come strumento investigativo*, in *Giurisprudenza Penale* WEB, 11, 2021, disponibile online; Si veda anche G. TODARO, *Op. loc. cit.* A tal proposito, merita particolare attenzione l'Accordo PNR tra Unione Europea e Canada.

40. Entrambi gli aspetti incidono sulla soluzione proporzionata che si fonda su un equilibrato contemperamento di interessi giuridicamente rilevanti, garantendo la realizzazione di ciascuno senza che uno prevalga sull'altro. La raccolta e l'analisi dei dati PNR, finalizzate alle indagini e alla prevenzione dei reati, legittimano di per sé l'obiettivo perseguito dalla Direttiva PNR, ossia il contrasto alla criminalità e la tutela della sicurezza pubblica. Tuttavia, per valutare se l'ingerenza temporale sia effettivamente limitata al minimo indispensabile, risulta imprescindibile stabilire un limite temporale rigoroso per la conservazione dei dati e un criterio oggettivo che circoscriva e monitori l'accesso e l'utilizzo delle informazioni, anche da parte di eventuali terzi. Sul punto, si v. B. PIATTOLI, *Principio di proporzionalità UE e trattamento dei dati personali nella lotta al terrorismo*, in *Diritto penale e processo*, n. 7, 2015, p. 892. Per un approfondimento, D.U. GALETTA, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Giuffrè, Milano, 1998, e A. SANDULLI, *La proporzionalità dell'azione amministrativa*, Cedam, Verona, 1998; F.G. SCOCA, *La discrezionalità nel pensiero di Giannini e nella dottrina successiva*, in *Riv. trim. dir. pubbl.*, n. 4, 2000; F. TRIMARCHI BANFI, C*anone di proporzione e test di proporzionalità nel diritto amministrativo*, in *Dir. proc. mmm.*, 2, 2016, p. 362; L. TORCHIA, *La dinamica del diritto amministrativo. Il principio di proporzionalità dell'azione amministrativa* (A. AVERARDI, S. DEL GATTO) in il Mulino, 2017, p. 68; F. G. SCOCA, L. LAMBERTI, *Valutazioni tecniche tutela del patrimonio culturale e principio di proporzionalità*, in *Federalismi*, n. 22, 2023, p. 224 ss.

41. Nel Parere 1/15 della Corte di Giustizia dell'Unione Europea, i giudici di Lussemburgo, pur riconoscendo in via

Tra le diverse tecniche utilizzate, quella del riconoscimento facciale ha riscosso rapidamente un notevole successo, suscitando l'interesse non solo delle forze dell'ordine e della pubblica amministrazione, ma anche di aziende interessate alle sue applicazioni nel campo della sicurezza e del *profiling*.[42]

I sistemi di identificazione e di verifica facciale si basano su una serie di procedimenti algoritmici che consentono di identificare una persona a partire dall'immagine del suo volto, utilizzando foto e video per risalire alla sua identità.[43]

teorica la sorveglianza di massa come uno strumento potenzialmente idoneo a prevenire attacchi terroristici e a garantire la sicurezza pubblica, hanno tuttavia censurato l'accordo internazionale tra Canada e Unione Europea relativo allo scambio di dati sul traffico aereo. Corte di giustizia dell'Unione europea, A-1/15, 26 luglio 2017. Si v. A. VERDASCHI, *L'accordo interazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di Giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 1° agosto 2017, 4, p. 1913. Per altri approfondimenti, si v. ID., *I programmi di sorveglianza di massa nello Stato di diritto. La 'data retention' al test di legittimità*, in *Diritto Pubblico Comparato ed Europeo*, 2014, p. 1224 ss; M. DICOSOLA, *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014; S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista Italiana di Diritto Pubblico Comparato*, 3-4, 2015, p. 819 ss; S. VILLANI, *Some Further Reflections on the Directive (EU) 2016/681 on PNR Data in the Light of the CJEU Opinion 1/15of 26 July 2017*, in *Revista de Derecho Político*, n. 101, 2018, p. 899 ss. Per altri approfondimenti, si consiglia la lettura della Relazione della Commissione al Parlamento Europeo e al Consiglio sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, disponibile online.

42. In alcune scuole, il riconoscimento facciale è stato utilizzato per monitorare l'accesso a studenti e visitatori, permettendo di individuare rapidamente eventuali potenziali rischi per la loro sicurezza. Un esempio simile si riscontra nel settore dei trasporti: a Roma, presso l'aeroporto di Fiumicino, sono stati installati sistemi di sorveglianza in grado di rilevare le caratteristiche biometriche del volto dei passeggeri, garantendone l'identificazione attraverso l'acquisizione temporanea delle informazioni contenute nei documenti di riconoscimento e nelle carte di imbarco. Sul punto, S. DEL GATTO, *La Governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del Riconoscimento facciale*, in *Riv. Ital. Dir. Pubbl. Comunitario*, 1, 2023, p. 42. A riguardo, si v. D.P.R. 15 gennaio 2018, n. 15, ovvero il Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia.

43. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, p. 65 ss. "Si ricorre sempre più frequentemente a questi dati biometrici non solo per finalità d'identificazione o come chiave per l'accesso a diversi servizi, ma anche come elementi per classificazioni permanenti, per controlli ulteriori rispetto al momento dell'identificazione o dell'autenticazione/verifica, cioè della conferma di una identità" così S. RODOTÀ, *Il diritto di avere diritti*, Bari-Roma, 2012, p. 302. Per altri approfondimenti, si v. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 3, 2021, p. 415 ss; A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) *Intelligenza artificiale e diritto: una rivoluzione? I diritti fondamentali dati personali e regolazione*, Bologna, 2022.

L'uso di sistemi di sorveglianza tramite il riconoscimento facciale solleva specifici problemi di tutela della privacy. A differenza di altri dati biometrici, come il DNA o le impronte digitali, questa tecnologia non sempre richiede il consenso esplicito dell'interessato. In molti casi, l'utente non è pienamente consapevole della raccolta delle proprie immagini, venendo, in alcune circostanze, spinto a fornire un consenso implicito o forzato, presentato come condizione imprescindibile per accedere a determinati servizi, cosa che riduce in modo significativo la sua libertà di scelta.[44]
A questo riguardo, rappresenta un esempio emblematico il caso che ha coinvolto la compagnia aerea Ryanair.
L'Autorità di controllo irlandese, il *Data Protection Commission*, ha avviato un procedimento istruttorio nei confronti della linea aerea, contestando l'uso della tecnologia di riconoscimento facciale per la verifica dell'identità dei passeggeri che prenotano voli tramite intermediari o portali di terze parti.[45] In particolare, durante la prenotazione di un volo tramite canali intermediari, agli utenti veniva richiesto di sottoporsi ad una procedura di verifica tramite riconoscimento facciale. Questa misura rendeva più complessa la fruizione del servizio, scoraggiando le prenotazioni attraverso terzi e spingendo i clienti ad utilizzare direttamente il sito ufficiale.
La procedura adottata, sebbene presentata dalla compagnia come un sistema volto a garantire una maggiore sicurezza e autenticità nelle prenotazioni, ha sollevato numerosi dubbi sul rispetto dei principi di liceità, trasparenza e minimizzazione del trattamento dei dati.[46]

44. Sulla mancata consapevolezza del consenso al riconoscimento facciale, si v. P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, GFL, Milano, 2020, p. 144. Per altri approfondimenti, si v. L. TORCHIA, *Op. loc. cit.* Tra i tipi di software biometrico, si includono il riconoscimento della voce, delle impronte digitali e della retina. L'immagine utilizzata in una procedura di riconoscimento facciale costituisce un dato biometrico di cui all'art. 4, par. 14, GDPR "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici". G. MOBILO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche*, n. 224, 2021, p. 12 ss. Sul riconoscimento facciale, il nuovo Regolamento Europeo sull'intelligenza artificiale, Considerando 14, "La nozione di "dati biometrici" utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del Regolamento (UE) 2016/679, all'articolo 3, punto 18, del Regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche".

45. Per ulteriori approfondimenti, si v. AGCM, Bollettino n. 15 del 15 aprile 2024, 8 ss.; Cfr. doc. 162, dati di traffico 2022 e 2023 forniti da ENAC lo scorso 14 febbraio; Per ulteriori approfondimenti, si v. A. RAMPANELLI, *Diritti dei passeggeri nel mercato aereo tra libera concorrenza e trasparenza tariffaria: brevi note a margine del caso Ryanair c. AGCM*, in *European Papers*, 13/06/2020, disponibile online.

46. Per maggiori approfondimenti, si v. *Data Protection Commission launches inquiry into Ryanair's Customer Verification Process*, in https://www.dataprotection.ie/en, disponibile online. E. RAFFIOTTA, M. BARONI, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal*, 1, 2022, p. 165 ss. Art. 9, co. 2, lett. g, GDPR. Per un caso analogo, si rimanda a M. MOLÉ, *Surveiller et punir: Amazon Francia e la sanzione del Garante dei dati per la sorveglianza "intrusiva e pressante" dei suoi magazzinieri*, in *Diritto delle Relazioni Industriali*, 2, 1° giugno 2024, p. 553.

In risposta alle crescenti preoccupazioni sollevate dai consumatori e all'indagine avviata, la compagnia aerea irlandese ha ribadito che le sue procedure di verifica sono finalizzate a tutelare i clienti da rischi connessi a potenziali frodi associate all'uso di canali non ufficiali. Inoltre, la compagnia ha precisato che tali pratiche sono pienamente conformi alle normative europee in materia di protezione dei dati personali.

Appare chiaro che l'implementazione di sistemi altamente invasivi, come il riconoscimento facciale per la conferma di prenotazioni o transazioni online, sollevi interrogativi significativi sotto il profilo della tutela della privacy, del rischio di discriminazione e del potenziale abuso per finalità di sorveglianza massiva. L'obbligatorietà di tali procedure può risultare non proporzionata rispetto ai benefici effettivamente conseguiti, specialmente considerando l'esistenza di soluzioni alternative meno invasive come l'autenticazione tramite codice OPT o documenti di identificazione tradizionali.

Questo scenario evidenzia la necessità di una riflessione critica sull'adeguatezza e la proporzionalità delle tecnologie biometriche nel contesto dei servizi digitali al fine di garantire un equilibrio tra innovazione e rispetto dei diritti fondamentali.

Nel panorama giuridico contemporaneo l'urgenza di ripensare l'interazione tra innovazione tecnologica e tutela dei diritti fondamentali ha subito una definitiva accelerazione con il divagare dell'intelligenza artificiale (AI).[47]

L'eccezionale progresso in questo ambito deriva dalla sinergia tra la disponibilità massiva di dati e una capacità computazionale in continua espansione, ulteriormente amplificata dall'adozione di sistemi intelligenti; uno scenario che, come anticipato nei precedenti paragrafi, solleva implicazioni di vasta portata per i diritti individuali, richiedendo un'approfondita revisione del *corpus* normativo elaborato dal costituzionalismo moderno.[48]

In risposta a queste sfide e alla crescente consapevolezza dei rischi insiti nell'uso dell'AI, il Regolamento Europeo sull'Intelligenza Artificiale rappresenta un intervento normativo di portata storica. La sua elaborazione è il frutto di un articolato processo preparatorio segnato dall'adozione di diversi atti di *soft law*, che hanno contribuito a costruire un quadro giuridico progressivo in materia di intelligenza artificiale.[49]

47. A. PIN, L. SCAFFARDI, *Op. loc. cit.*; Per altri approfondimenti, si v. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2, 2018, p. 65 ss; M. GRANIERI, *Una sinopsi comparativa e una prospettiva critica sui tentativi di regolazione dell'intelligenza artificiale*, in *Comp. dir. civ.*, 2, 2023, p.705; S.A. Di CAPRIGLIA, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionali, statunitense e sinico. Uno studio comparato*, in *Federalismi*, 9, 2024; L. CASINI, I*l futuro dello Stato Digitale*, in *Rivista Trimestrale di Diritto Pubblico*, 2, 2024, p. 431; L. LAZZERONI, *Lavoro e tutele nella dimensione della cittadinanza digitale e nell'era del capitalismo della sorveglianza*, in D*iritto delle Relazioni Industriali*, 3, 2024, p. 715; J. P. SOLÉ, *Il Regolamento dell'Unione Europea sull'intelligenza artificiale, La discrezionalità amministrativa e la riserva di umanità*, in *Rivista Trimestrale di Diritto Pubblico*, 3, 2024, p. 825.

48. R. BIFULCO, *Intelligenza artificiale, internet e ordine spontaneo*, in F.PIZZETTI, *Op. loc. cit.*, p. 383 ss.

49. Tra i più rilevanti, meritano particolare attenzione le Risoluzioni del Parlamento Europeo del 20 ottobre 2020,

Tra le tappe fondamentali di questo percorso, il Libro Bianco sull'AI, pubblicato nel febbraio del 2020, ha svolto un ruolo cruciale nel definire un approccio integrato volto a coniugare l'eccellenza tecnologica con la fiducia pubblica: da un lato ha incoraggiato lo sviluppo di sistemi di intelligenza artificiale affidabili, sicuri ed eticamente sostenibili; dall'altro ha evidenziato la necessità di creare un ecosistema digitale che fosse non solo tecnicamente solido, ma anche capace di garantire inclusione sociale e competitività economica dell'Unione Europea.[50]

Per promuovere un quadro normativo armonizzato in tutto lo Spazio Europeo, si è optato per l'adozione di un regolamento piuttosto che di una direttiva, seguendo una logica analoga a quella applicata per il GDPR.

Nonostante ciò, in un ambito così dinamico come l'intelligenza artificiale, questa impostazione pone sfide significative derivanti dalla continua evoluzione tecnologica e dalla natura autonoma e imprevedibile dei sistemi più avanzati.[51]

Consapevole di queste complessità, la normativa integra meccanismi di flessibilità volti a garantire l'aggiornamento e l'adattabilità delle regole nel tempo, al fine di fronteggiare l'estrema variabilità delle applicazioni dell'AI e i rischi emergenti, non sempre prevedibili *ex ante*.[52]

Questo è reso evidente dall'adozione di un approccio proporzionato, basato sulla valutazione del rischio connesso all'automazione delle decisioni e, più in generale, all'uso dell'intelligenza artificiale, prevedendo obblighi e misure differenziati e modulati in base alla potenziale gravità dell'entità del rischio.

In particolare, i sistemi a rischio inaccettabile sono soggetti a un divieto generale, salvo deroghe esplicite, a causa del loro potenziale di ledere gravemente i diritti fondamentali; i sistemi ad alto rischio costituiscono il fulcro della disciplina, con l'impostazione di stringenti requisiti di trasparenza, sicurezza e supervisione umana; infine, i sistemi a basso e minimo rischio, pur essendo

dedicate rispettivamente ai principi etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, e al regime di responsabilità civile per l'AI. Sul punto, si v. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal Rivista di BioDiritto*, n. 3, 2021, p. 416.

50. Per altri approfondimenti, si v. F. RODI, *Gli interventi dell'Unione europea in materia di intelligenza artificiale e robotica: problemi e prospettive*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, 2020, p. 187-210.

51. Sul punto, si v. C. CASONATO, B. MARCHETTI, *Op. loc. cit.* che richiamano le celebri parole di R. POUND, *Interpretations of Legal History*, Cambridge, 1923 "Law must be stable, and yet it cannot stand still". Tale affermazione sintetizza la necessità di equilibrio tra la stabilità normativa e l'evoluzione del diritto, imprescindibile per rispondere alle mutevoli esigenze della società.

52. In questo contesto, appare rilevante richiamare le riflessioni del Professor Oreste Pollicino, il quale osserva come l'AI Act (analogamente al GDPR), si presenti formalmente come un regolamento direttamente applicabile, ma includa al suo interno una serie di clausole aperte, attribuendo agli Stati membri un significativo margine di discrezionalità. Secondo il professor Pollicino, ciò rende l'AI Act una sorta di "direttiva mascherata", che coniuga uniformità normativa e flessibilità di attuazione a livello nazionale. *L'AI Act sarà una direttiva mascherata. Dialogo con Pollicino (Bocconi)*. Disponibile online al seguente link: https://www.iaic.it/news/lai-act-sara-una-direttiva-mascherata-dialogo-con-pollicino-bocconi/.

essenzialmente esenti da vincoli severi sono soggetti ad obblighi minimi di informazione volti a garantire la consapevolezza degli utenti e una gestione trasparente dei dati.
La tecnologia di riconoscimento facciale è inclusa nei sistemi ad alto rischio a causa del suo impatto potenzialmente significativo sui diritti fondamentali e sulla privacy degli individui; un rischio particolarmente rilevante che potrebbe verificarsi quando applicata per l'identificazione biometrica remota in spazi pubblici, sollevando questioni di trasparenza, sorveglianza di massa e controllo sociale.[53]
A riguardo, il Regolamento sull'Intelligenza Artificiale introduce una chiara distinzione tra i sistemi di identificazione biometrica "in tempo reale" e quelli "a posteriori".[54]
I sistemi di identificazione biometrica "in tempo reale" elaborano dati generati dal vivo o quasi dal vivo, acquisiti tramite telecamere o dispositivi analoghi, al fine di identificare gli individui in modo immediato. Tali sistemi trovano impiego, ad esempio, in ambiti di sorveglianza pubblica o per esigenze di pubblica sicurezza, in cui la tempestività dell'identificazione è cruciale per prevenire o gestire situazioni di rischio. I sistemi di identificazione biometrica "a posteriori", invece, processano dati biometrici acquisiti precedentemente, come immagini o video registrati, consentendo il processo di confronto e di identificazione degli individui con un ritardo temporale significativo rispetto alla raccolta dei dati.[55]

53. "Adoperando un parallelo letterario, si potrebbe sostenere che il problema non nasca soltanto – richiamando la già citata metafora orwelliana del Grande Fratello – dalla sorveglianza in sé, il controllo sociale e la capacità inibitoria che ne deriva; quanto piuttosto – prendendo in prestito la metafora kafkiana de "Il processo" – la sottoposizione ad un potere invisibile e incomprensibile che può raccogliere informazioni su ciascuno, compilare profili e dossier, assumere decisioni senza fornire spiegazioni o garantire alcuna partecipazione." Così G. MOBILIO, *Op. loc. cit*, p. 21. Per altri approfondimenti, si v. Per altri approfondimenti, si v. S. ZUBOFF, *Il Capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019; R. DUCATO, *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L.E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, 2021, p. 187 ss; Per altri approfondimenti, si v. M.ALLENA, S. VERNILE, *Intelligenza artificiale trattamento di dati personali e pubblica amministrazione* in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) *Op. cit.*, p. 389 ss.; D.U.GALETTA, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *Federalismi*, 5, 2023; A. PIN, L. SCAFFARDI, *Tra la protezione dei dati e intelligenza artificiale, in Europa e oltre*, in *Sezione Monografica: Le sfide della protezione dei dati personali di fronte all'intelligenza artificiale: un approccio comparato*, in *DPCE: online*, 2, 2024, p. 1029. Cfr. Considerando n. 15 ss.
54. Tra le disposizioni rilevanti in materia di identificazione biometrica, si segnalano: l'Allegato III che elenca i settori e le applicazioni ad alto rischio; l'art. 5 relativo al divieto di pratiche invasive, salvo in specifiche circostanze eccezionali, l'art. 52 che disciplina gli obblighi di trasparenza e l'art. 71 riguardante la sorveglianza e il monitoraggio.
55. L'Art. 10, co. 10, par. 2, della normativa sancisce che il sistema di identificazione biometrica remota a posteriori non può essere utilizzato per attività di contrasto in modo indiscriminato. È consentito esclusivamente se vi è un legame con un reato, un procedimento penale, una minaccia concreta e attuale o una previsione specifica di reato. Inoltre, è escluso l'uso di tale sistema per la ricerca di persone scomparse.

5. Considerazioni conclusive: il rischio del Panopticon Digitale

Questa complessa cornice regolatoria solleva significative riflessioni di ordine etico, giuridico e sociale, portando alla luce il potenziale rischio di una trasformazione delle dinamiche di sorveglianza in un panopticon digitale.
Il concetto di Panopticon, originariamente ideato dal filosofo Jeremy Bentham come un sistema che permette una sorveglianza onnipresente ma invisibile, è stato successivamente ripreso da Michel Foucault per descrivere un modello di potere disciplinare diffuso nella società moderna.
Il panopticon non si limita al controllo fisico, ma diviene un paradigma per una sorveglianza continua capace di influenzare il comportamento degli individui, talvolta anche in assenza di una effettiva osservazione.
Nell'era digitale, questa idea trova una declinazione attraverso le tecnologie di sorveglianza biometrica e sistemi di monitoraggio algoritmico.
L'identificazione biometrica, quale il riconoscimento facciale, la scansione dell'iride o l'analisi delle impronte digitali, consente un controllo capillare e pervasivo, trasformando i cittadini in oggetti di una osservazione permanente. In particolare, i sistemi "in tempo reale", incarnano questo rischio in modo evidente: la possibilità di monitorare e identificare immediatamente gli individui in spazi pubblici può creare un clima di sorveglianza permanente, dove la libertà personale e il diritto alla privacy rischiano di essere subordinati alle esigenze di sicurezza.
L'effetto deterrente di tali tecnologie potrebbe condizionare il comportamento sociale, inducendo una forma di autocensura collettiva analoga a quella descritta da Foucault, in cui la semplice consapevolezza di essere potenzialmente osservati modifica le azioni degli individui.
Anche i sistemi *ex post* pongono questioni di rilievo, anche se meno immediate. La registrazione di dati da utilizzare a posteriori pone potenzialmente molteplici problemi, che attengono principalmente alla proporzionalità e, di conseguenza, alla legittimità del trattamento dei dati nel tempo.
L'accumulo di tali informazioni rischia di condurre ad uno scenario in cui gli individui sono costantemente monitorati in modo retrospettivo, erodendo ulteriormente la linea di demarcazione tra sorveglianza giustificata e un potenziale abuso del potere tecnologico.
Soltanto un approccio olistico, in grado di bilanciare sicurezza e libertà, può garantire che l'innovazione tecnologica sia messa al servizio della società, odierna e futura, senza comprometterne i fondamenti democratici.
In conclusione, volendo trarre una qualche considerazione, emerge con chiarezza come questo tema, ancora in fase di definizione e al centro di un intenso dibattito sia a livello dottrinario che giurisprudenziale, si inserisca nel più ampio contesto della cosiddetta "sfida dei dati"; una questione di rilevanza globale che coinvolge non solo l'Europa, ma l'intero panorama internazionale, evidenziando preoccupazioni comuni nell'ambito del continuo tentativo di sviluppare gli strumenti necessari a garantire la qualità e la sicurezza dei servizi basati sull'intelligenza artificiale, aventi altresì implicazioni durature per le generazioni future.