

La *privacy* nell'era dell'intelligenza artificiale

di Tommaso Edoardo Frosini

Abstract: *Privacy in the age of artificial intelligence*— The right to privacy today has its own particular conformation, just with reference to the needs of protection that can occur through the Internet. In particular, with artificial intelligence, new legal issues referring to privacy may arise. This is what is addressed and discussed in this article. The conclusion, however, is that it does not seem that the EU Regulation (GDPR) is compatible with current models of data flow management, which generate algorithms through which decisions are made in various scientific fields. The article closes with a provocation: it is possible to imagine that on the basis of big data an algorithm could be elaborated that would be able to detect privacy violations, especially the one that deserves more attention and concern: the so-called sensitive data. It would be enough that every time the algorithm identifies a sensitive data processed without the consent of the person concerned, it activates a preventive action of blocking the procedure or a subsequent action with the prescription of a sanction for the violation of the law.

273

Keywords: Privacy; Artificial Intelligence; Algorithm; Big Data.

1. Come cambia il right to privacy

C'era una volta il *right to privacy*. Venne concepito nel 1890 sulle colonne della prestigiosa *Harvard Law Review*; gli autori, due giovani giuristi statunitensi, Samuel Warren e Louis Brandeis, teorizzarono il diritto alla *privacy* da intendersi come *right to be let alone*¹. L'occasione per elaborare ed enunciare il *right to privacy* venne data da un episodio, accaduto nell'America di quegli anni. La vicenda è nota, ma vale la pena rievocarla brevemente anche perché ancora di attualità (specialmente e di recente in Italia ...). Samuel Warren, un giovane avvocato, aveva sposato la figlia del ricco bostoniano Byard, e aveva iniziato a condurre una fastosa e festosa vita di società, con ricevimenti del genere che una generazione dopo G. Scott Fitzgerald avrebbe reso celebre con i suoi romanzi. La stampa locale diede largo risalto, nelle cronache mondane, a quei festini, che parevano ricchi di ostentazione finanziaria, facendo anche qualche considerazione poco benevola su quello spreco di denaro. Warren si associò all'avvocato Brandeis

¹ S. Warren, L. Brandeis, *The right to privacy*, in *Harvard Law Review*, 5, 1890, 193-220: trad.it. nel vol. *Jus solitudinis*, a cura e con intr. di V. Frosini, Milano 1993 (edizione fuori commercio quale "Strenna natalizia Giuffrè"), 53 ss.

(che sarebbe diventato, anni dopo, giudice della Corte Suprema), scrissero l'articolo e avviarono un'azione legale per protestare contro l'invasione della stampa e per invocare dalle Corti di giustizia il rispetto della sua vita privata. Non si chiedeva però di esaltare la difesa della solitudine fisica, piuttosto di ricondurre la *privacy* alla tutela dei valori di autonomia e dignità dell'individuo, che comprendono anche la protezione della sua cerchia familiare e persino di quella societaria, in cui egli ha scelto di collocarsi.

Il *right to privacy* non trovò, però, immediata tutela presso le Corti americane; anche la Corte Suprema non lo volle accogliere nel famoso caso *Olmstead* del 1928, dove però nella sentenza comparve un'importante *dissenting opinion* del giudice Brandeis (lo stesso che aveva scritto, insieme a Warren, l'articolo sopra ricordato). Fu nel 1965, con il caso *Griswold*, che la Corte Suprema riconobbe ed elaborò il diritto costituzionale alla *privacy*, quale fondamento dei diritti di libertà dell'individuo (libertà personale, di manifestazione del pensiero, di comunicazione e così via)². Da quella pronuncia in poi, il diritto costituzionale alla *privacy* ha trovato un forte radicamento nella cultura giuridica statunitense, al punto da diventarne uno dei pilastri della stessa, caratterizzandone sempre più la sua matrice liberale. Il seme della *privacy* lanciato dall'America ha trovato terreno fertile in Europa e, sia pure tardivamente, anche in Italia. Non è certo questa la sede per svolgere una compiuta ricostruzione della nascita e poi dello sviluppo del diritto alla *privacy* negli ordinamenti europei³. Vorrei però quantomeno evidenziare uno dei motivi di evoluzione della concezione della *privacy*, non più e non tanto come “diritto a essere lasciati soli”, e quindi una forma passiva di tutela, piuttosto anche come “diritto a disporre dei propri dati”, assumendo pertanto una forma attiva di partecipazione informativa. Infatti, e soprattutto con l'avvento dei *computer* prima e di Internet dopo, la problematica riguarda non tanto il controllo delle informazioni individuali in difesa di un diritto del soggetto alla riservatezza, quanto piuttosto il metodo adottato per la raccolta dei dati, ossia la possibilità di raccogliere le informazioni in una “banca dati” elettronica⁴. Da qui, la nuova esigenza di tutelare la riservatezza dei dati personali, ovvero di impedire che notizie

² Le vicende giurisprudenziali statunitensi sono descritte da A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974. V. ora la raccolta delle decisioni della Corte Suprema: *The Right to Privacy. Historic US Supreme Court Decisions*, 2012 (Ebook Kindle)

³ Su cui, v. ora A. Di Martino, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Napoli, 2017. Oggi si assiste a una significativa distinzione fra la tutela della *privacy* in UE e in USA, originata anche da alcune pronunce della Corte UE: il tema è di sicuro interesse e varrebbe la pena approfondirlo, non è però questa la sede per farlo. Comunque, per una prima valutazione del problema, cfr. E. Terioli, *Privacy e protezione dei dati personali Ue vs. Usa. Evoluzioni del diritto comparato e il trasferimento dei dati dopo la sentenza “Schrems II”*, in *Dir. Inf.*, 1, 2021, 49 ss.

⁴ In tema di diritto alla *privacy*, con riferimento alle problematiche presenti e future derivanti dall'uso (o abuso) dei dati elettronici, cfr. T.E. Frosini, *Le sfide attuali del diritto ai dati personali*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, 25 ss.

riguardanti la sfera intima della persona possano essere divulgate e conosciute da terzi, con il rischio che questo possa procurare forme di discriminazione. Si pensi ai dati sanitari o sessuali, e quindi alla possibilità che la conoscenza di questi possa consentire un trattamento discriminatorio nei confronti di chi è affetto da una certa malattia oppure le cui scelte sessuali sono diversificate. Anche se, proprio su quest'ultimo aspetto, si assiste, da ultimo, anche a una voluta recessione della *privacy*, a seguito di una crescente legislazione, nei Paesi di democrazia liberale, volta a dare pieno riconoscimento ai vari modi di esprimere liberamente le proprie inclinazioni sessuali. In tal modo, non si vuole più ricorrere a un diritto di riservatezza, che finirebbe con l'essere percepito come una sorta di "nascondiglio", invece come diritto di libertà alla propria identità sessuale. Certo, la questione non può dirsi ancora pienamente risolta in questi termini, e non può nemmeno essere affrontata qui in forma approfondita come merita.

Il diritto alla *privacy* oggi ha una sua particolare conformazione, proprio con riferimento alle esigenze di tutela che possono prodursi attraverso la rete Internet. Provo a fare degli esempi con riferimento a *provider* o motori di ricerca a tutti noti: *Amazon* monitora le nostre preferenze d'acquisto; *Google* registra le nostre abitudini in Rete; *Facebook* conosce le nostre relazioni sociali e ciò che *like*; gli operatori di telefonia mobile fanno non solo con chi parliamo, ma anche chi si trova nelle vicinanze. Lasciamo impronte elettroniche ovunque: da queste, infatti, si può risalire per sapere cosa abbiamo acquistato, in quale località siamo stati, dove e cosa abbiamo mangiato e così via. Da qui il progressivo formarsi di una tendenziale società sorvegliata, dove l'insieme delle relazioni sociali che si svolgono in rete sono naturalmente tracciabili⁵.

Sul diritto alla *privacy*, quindi, c'è un prima e un dopo. Il confine è segnato dall'avvento di Internet, databile a partire dal secolo Ventunesimo. Perché un conto sono i dati personali raccolti e custoditi in apposite banche dati, di cui però c'è, almeno formalmente, un responsabile della gestione delle stesse, sebbene il problema sia quello del flusso dei dati da una banca all'altra, un conto è Internet e la sua capacità di diffondere, subito e in tutto il mondo, dati che si riferiscono a una singola persona ovvero a imprese pubbliche e private. È chiaro che Internet consente un flusso sterminato di dati il cui controllo appare difficile regolare. La questione oggi è resa più complessa con i cd. *big data*⁶: si tratta dell'accumulo enorme di dati, tale da inondare il mondo di informazioni come mai prima d'ora, con una continua e irrefrenabile crescita. Il cambiamento di dimensione ha prodotto un cambiamento di stato. Il cambiamento quantitativo ha prodotto un

⁵ S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tr.it., Roma, 2019.

⁶ Da ultimo, V. Zeno Zencovich, *Big data e epistemologia giuridica* e A. Stazi, *Legal big data: prospettive applicative in ottica comparatistica*, entrambi nel vol. S. Faro, T.E. Frosini, G. Peruginelli (a cura di) *Dati e algoritmi. Diritto e diritti nella società digitale*, cit., 13 ss. e 77 ss.

cambiamento qualitativo. Sono state l'astronomia e la genomica, che per prime hanno sperimentato l'esplosione dei dati, a coniare l'espressione "big data". E adesso il concetto si sta espandendo a tutti gli ambiti della vita umana. Pertanto, si tratta delle cose che si possono fare solo su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi, e altro ancora. Faccio un esempio, riferito a Internet: *Google* processa oltre 24 *petabyte* di dati al giorno, un volume pari a mille volte la quantità di tutto il materiale a stampa contenuto nella biblioteca del Congresso degli Stati Uniti. Su *Facebook*, un'azienda che fino a una decina di anni fa nemmeno esisteva, si caricano ogni ora oltre dieci milioni di nuove fotografie. Gli iscritti a *Facebook* cliccano sul pulsante *I like* o lasciano un commento quasi tre miliardi di volte al giorno, creando un percorso digitale che l'azienda può analizzare per capire le preferenze degli utenti. È questo il punto: la possibilità per le grandi aziende di Internet di elaborare un'identità digitale degli utenti da utilizzare a scopi commerciali o politici.

È nota la recente vicenda che ha coinvolto *Facebook* per avere ceduto a una società di ricerche, *Cambridge Analytica*, i dati dei suoi utenti per consentire un trattamento finalizzato a individuare categorie di elettori. Questo dipenderebbe dai *like* che mettiamo sui *social*, come per esempio *Facebook* o *Twitter*. Perché ogni *like* che lasciamo sui *social* sarebbe un tassello in una sorta di auto-schedatura volontaria di massa, che finirebbe con offrire opportunità e poteri a chi vuole orientare le opinioni. Studi condotti da psicologi, peraltro, sostengono che bastano sessantotto *like* di un utente *Facebook* per individuare il colore della sua pelle (con precisione pari al 95%), l'orientamento sessuale (88%) e quello politico (85%). Quindi, le opinioni politiche sono conosciute da *Facebook*; quindi, il voto non è più segreto. È chiaro che questo aspetto va a colpire un diritto costituzionale quale quello del diritto di voto. E va altresì a colpire la riservatezza del cittadino laddove si individua la sua scelta politica, che è un dato sensibile che dovrebbe essere tutelato al massimo livello⁷. È una nuova forma di potere, quello dei *provider* di assecondare i gusti di ciascuno sulla base di ciò che fanno di noi.

Ancora, e sempre in tema di diritto alla *privacy* e Internet. Si pensi ai recenti scandali internazionali, che sono stati sollevati con riferimento alla capacità di uno Stato di gestire i dati personali di migliaia di persone influenti, che appartengono e rappresentano le istituzioni europee. Ovvero l'indisponibilità personale dei dati che viaggiano sul *cloud computing*, laddove tutto il nostro patrimonio informativo finisce per essere sottratto alla nostra indisponibilità e per risiedere in *server* posti al di fuori del nostro controllo diretto, e quindi potenzialmente esposti a violare la nostra *privacy*. Il problema, peraltro, riguarda non solo dati personali, ma soprattutto grandi banche dati di operatori telefonici, imprese, istituti di credito e di risparmio,

⁷ Sulla questione, v. T.E. Frosini, *Internet e democrazia*, in *Dir. Inf.*, 4-5, 2017, 657 ss. (ora in Id., *Liberté Égalité Internet*, 2° ed., Napoli, 2019, 211 ss.).

che hanno un indubbio valore strategico. I dati, e la loro libera circolazione, rappresentano un sicuro volano per lo sviluppo economico e il progresso sociale degli Stati e dei loro cittadini⁸.

Quindi, l'«orizzonte giuridico dell'Internet», come è stato definito⁹, continua sempre più ad allargare e ampliare il suo panorama teorico e pratico. E si aprono nuovi scenari in punto di diritti fondamentali, quale il diritto di libertà di manifestazione del pensiero, il cui significato occorre rifondare alla luce delle sue nuove implicazioni d'ordine giuridico¹⁰. Le nuove frontiere del diritto e dei diritti oggi sono rappresentate dalle potenzialità della intelligenza artificiale (d'ora in poi: A.I., secondo l'acronimo inglese), ovvero dalla enorme capacità di raccogliere, sistematizzare ed elaborare dati per produrre algoritmi in grado di trovare soluzioni "intelligenti" per risolvere problemi, oppure per assumere decisioni autonomamente e imparzialmente¹¹. Si è avverata così la profezia di J.W. Goethe, espressa nel *Faust* a inizi Ottocento: «E così ci sarà un pensatore, che costruirà un cervello che sappia pensare esattamente» (atto II, versi 6869-6870).

La A.I. impatta su tutte le scienze del sapere umano declinandole artificialmente. Anche il diritto, che dovrà sempre più rimodularsi nei suoi paradigmi, tenendo conto dell'uso degli algoritmi per concorrere a migliorare le pronunce giurisdizionali ovvero per elaborare neutrali atti amministrativi, per citare solo alcuni esempi¹². Certo, il diritto già da tempo è entrato nella società tecnologica – ovvero cibernetica, come veniva chiamata e come ora viene opportunamente riproposta¹³ – con tutti i suoi temi e problemi derivanti dall'applicazione delle tecniche giuridiche, sostanziali e processuali, nel vasto mondo della tecnologia e i suoi derivati, in particolare la rete Internet. Pertanto, si potrebbe riformulare l'antico brocardo latino con *ubi societas tecnologica, ibi ius*. Si assiste, a seguito dell'affermarsi della tecnologia, a un nuovo modo di essere del diritto e, conseguentemente, a un processo di metamorfosi della figura del giurista come umanista in quella del giurista tecnologico. Il cui compito è quello di farsi interprete delle trasformazioni che si stanno verificando nella società

⁸ È questa la tesi di T. Ramge, V. Mayer-Schönberger, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, tr.it., Milano, 2021.

⁹ V. Frosini, *L'orizzonte giuridico dell'Internet*, in *Dir. Inf.*, 2, 2000, 271 ss.

¹⁰ Sulle cui problematiche, con riferimento all'era digitale, v. ora S. Sassi, *Disinformazione contro Costituzionalismo*, Napoli, 2021.

¹¹ Per un'analisi più approfondita delle peculiarità tecniche riguardanti l'AI si veda in questo fascicolo P. Traverso, *Breve introduzione tecnica all'Intelligenza Artificiale*.

¹² Per un quadro d'insieme, si v. il bel volume A. D'Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2020 (*ivi*, spec. i contributi di A. D'Aloia, C. Casonato, A. Simoncini e F. Donati).

¹³ V. Frosini, *Cibernetica diritto e società*, Milano, 1968; ripropone l'uso del termine "cibernetica", sottolineando l'affinità fra questa e il diritto, perché «entrambi mirano a studiare e a rendere prevedibili i modelli di comunicazione e controllo dei comportamenti collettivi»: così, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in A. D'Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 171.

sulla base dello sviluppo della tecnologia, e dell'impatto che questa sta avendo sul diritto, sui diritti. Emergono, infatti, dalla coscienza sociale, e a seguito dello sviluppo tecnologico, dei “nuovi diritti”, i quali, sebbene non godano di un loro esplicito riconoscimento normativo, hanno un forte e chiaro “tono costituzionale”, che li collocano, implicitamente, all'interno della costituzione, riservando all'interprete il compito di estrapolarli da essa, anche attraverso quella che ho chiamato una interpretazione tecnologicamente orientata¹⁴. Purtroppo bisogna essere consapevoli dei rischi che vi possano essere presunti vizi di incostituzionalità delle leggi che prevedono e prescrivono l'uso della AI, eventualmente riferibili alla cd. “discriminazione algoritmica”¹⁵.

2. Il diritto di libertà informatica, quale base per la privacy che cambia

Prima però di avviarmi sul percorso interpretativo del diritto alla *privacy*, con riferimento ai problemi applicativi derivanti dall'intelligenza artificiale, ritengo opportuno insistere su un tema che ritengo prodromico a tutte le questioni che concernono Internet e i suoi derivati tecnologici in punto di diritto, compreso quindi il diritto alla *privacy*. Anzi: un tema che andrebbe tenuto ben presente nelle riflessioni che si svolgono, nella letteratura giuridica, sul diritto nella società tecnologica, per così dire. Si tratta della dottrina della “libertà informatica”¹⁶. Una teoria che venne avanzata ed esposta nell'ormai lontano 1981 e che aveva la sua matrice ideologica nella concezione di un nuovo liberalismo, inteso come fermento lievitante di una civiltà liberale promossa dalla rivoluzione tecnologica; e si sviluppava sulla base di una nuova dimensione del diritto di libertà personale, in una fase storica della civiltà industriale caratterizzata dall'avvento di quelli che all'epoca venivano chiamati “calcolatori elettronici” (oggi *computers*). Tipico nuovo diritto scaturito dalla evoluzione della civiltà tecnologica, il diritto di libertà informatica manifesta un nuovo aspetto dell'antica idea della libertà personale e costituisce l'avanzamento di una nuova frontiera della libertà umana verso la società futura, e che si viene a collocare nel prisma del costituzionalismo contemporaneo¹⁷.

Nella sua originaria versione, quella esposta nel 1981, la libertà

¹⁴ T. E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Dir. Inf.*, 3, 2020, 465 ss.; v. anche C. Casonato, *Per una intelligenza artificiale costituzionalmente orientata*, in A. D'Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 131 ss.

¹⁵ Sul punto, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 196.

¹⁶ Cfr. la relazione di V. Frosini, *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), *Privacy e banche dei dati*, Bologna, 1981, 37 ss. (poi compresa nel vol. Id., *Informatica diritto e società*, 2a ed., Milano 1992, 173 ss.).

¹⁷ Cfr. T. E. Frosini, *Il costituzionalismo nella società tecnologica*, cit., 465 ss.; nonché Id., *Apocalittici o integrati. La dimensione costituzionale della società digitale*, Modena, 2021.

informatica veniva raffigurata – al pari di quella politica (secondo la dottrina di Isaiah Berlin) – come *positiva* e *negativa*. La libertà informatica negativa, esprime «il diritto di *non* rendere di dominio pubblico certe informazioni di carattere personale, privato, riservato (qualifiche queste, che potrebbero in certi casi non coincidere tra loro); la libertà informatica positiva, invece, esprime la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della *privacy* per essere divenuti elementi di *input* di un programma elettronico; e dunque libertà informatica positiva, o diritto soggettivo riconosciuto, di conoscere, di correggere, di togliere o di aggiungere dati in una scheda personale elettronica»¹⁸.

Ecco che così il diritto di libertà informatica assume una nuova forma del tradizionale diritto di libertà personale, come diritto di controllare le informazioni sulla propria persona, come diritto dello *habeas data*. L'evoluzione giurisprudenziale ha riconosciuto e affermato questo nuovo diritto di libertà nei termini di protezione dell'autonomia individuale, come pretesa passiva nei confronti dei detentori del potere informatico, dei privati o delle autorità pubbliche. Con la nuova legislazione sulla tutela delle persone rispetto al trattamento dei dati personali, prima nazionale ora eurounitaria con il Regolamento UE 2016/679 che ha codificato il *General Data Protection Regulation* (d'ora in poi: GDPR), la nozione del diritto di libertà informatica ha trovato riconoscimento nel diritto positivo; ma nel frattempo ha subito una trasformazione, giacché il diritto di tutelare i propri dati si attua nei confronti di qualunque trattamento di essi, anche non elettronico; e ha subito altresì un mutamento del suo carattere, prima ispirato al principio della difesa dinanzi al potere informatico, ora considerato come un diritto attivo di partecipazione del cittadino al circuito delle informazioni. Emerge così il problema del riconoscimento di un diritto all'identità personale come nuovo diritto della personalità, costituito dalla proiezione sociale della personalità dell'individuo cui si correla un interesse del soggetto a essere rappresentato nella vita di relazione con la sua vera identità¹⁹. La libertà di custodire la propria riservatezza informatica è divenuta anche libertà di comunicare ad altri le informazioni trasmissibili per via telematica, per esercitare così la libertà di espressione della propria personalità avvalendosi dei sistemi di comunicazione automatizzata.

Il diritto di libertà informatica acquisisce oggi un ulteriore significato a seguito dell'avvento di Internet, e ciò vale a dimostrare la sua attualità teorica²⁰. Infatti, con Internet, il diritto di libertà informatica «è diventato una pretesa di libertà in senso attivo, non libertà *da* ma libertà *di*, che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di

¹⁸ Così V. Frosini, *La protezione della riservatezza nella società informatica*, cit., 37 ss.

¹⁹ Da ultimo, G. Alpa, *Il diritto di essere se stessi*, Milano, 2021.

²⁰ Cfr. C. Castillo Jimenez, *Las nuevas tecnologías de la informacion y el derecho*. De Vittorio Frosini a Internet, Siviglia, 2003.

ogni genere. È il diritto di partecipazione alla società virtuale, che è stata generata dall'avvento degli elaboratori elettronici nella società tecnologica: è una società dai componenti mobili e dalle relazioni dinamiche, in cui ogni individuo partecipante è sovrano nelle sue decisioni»²¹. Ci troviamo di fronte, indubbiamente, ad una nuova forma di libertà, che è quella di comunicare con chi si vuole, diffondendo le proprie opinioni, i propri pensieri e i propri materiali, e la libertà di ricevere. Libertà di comunicare, quindi, come libertà di trasmettere e di ricevere. Vale la pena di citare l'art. 19 della Dichiarazione universale dei diritti dell'uomo dell'Onu, che così ha chiaramente precisato il diritto di libertà di manifestazione del pensiero: «cercare, ricevere, diffondere con qualunque mezzo di espressione, senza considerazione di frontiere, le informazioni e le idee». Formulazione perfetta, anche e soprattutto nell'era dell'Internet.

3. La UE e il bisogno di normare: considerazioni critiche

Assistiamo, quindi, a un profondo cambiamento del diritto alla *privacy*: non più diritto a essere lasciati soli, quello che è stato chiamato il diritto di Robinson Crusoe²², ma piuttosto il diritto a disporre dei propri dati, che circolano sulla rete. D'altronde, se non si potesse disporre dei propri dati, oggi si verrebbe esclusi da tutta una serie di attività, private e pubbliche; se è vero, come è vero, che siamo sempre più *on life*, dove non si distingue fra la vita reale e quella virtuale²³. Peraltro, i propri dati si gestiscono attraverso i numerosi *social network*, ovvero sulla rete internet con i suoi siti *web*. Pensare di soffocare questa evoluzione della libertà informatica, in nome di una concezione “datata” della *privacy*, vuol dire mettere un bavaglio al progresso tecnologico e alla cittadinanza digitale²⁴. Mi sembra, francamente, una posizione anacronistica e apocalittica²⁵. Basti tenere conto che si tratta, soprattutto, di un fatto generazionale, perché quelli che oggi hanno vent'anni sono la prima generazione che non conosce altra civiltà che quella digitale.

Se non proprio un bavaglio, comunque un limite all'espansione della società digitale oggi viene dalla UE, per via di un suo continuo interventismo normativo rivolto a “plasmare il futuro digitale dell'Europa”. A cominciare proprio dalla regolazione della *privacy* con il GDPR del 2016, che ha fissato regole comuni per i Paesi della UE relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi. E lo ha fatto con 173 “Considerando”, ai quali

²¹ Così V. Frosini, *L'orizzonte giuridico dell'Internet*, cit., 275; Id., *La democrazia nel XXI secolo*, Macerata, 2010, *passim*.

²² V. Frosini, *L'ipotesi robinsoniana*, in *Annali del seminario Giuridico* dell'Università di Catania, vol. VI-VII, Milano, 1953, 168 ss. (ora nel vol. *Jus solitudinis*, cit., 79 ss.).

²³ Il neologismo *on life*, che indica il fatto che siamo tutti sempre più connessi, è di L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009.

²⁴ Su cui, v. G. Pascuzzi, *La cittadinanza digitale*, Bologna, 2021.

²⁵ Per uno sviluppo argomentativo, v. T. E. Frosini, *Apocalittici o integrati. La dimensione costituzionale della società digitale*, cit.

seguono 99 articoli, suddivisi in 11 capi: quindi, una legge complessa e articolata²⁶. Ora la stessa UE si appresta a varare un regolamento sul *Digital Services Act* e sul *Digital Services Market* e, soprattutto, sulla AI²⁷. Al diritto scritto, poi, si deve aggiungere il diritto giurisprudenziale con i numerosi pronunciamenti della Corte di Giustizia UE sul diritto all'oblio, sul (divieto di) trasferimento di dati dalla UE agli USA, su *Facebook* e altro ancora²⁸. Stretto in una morsa giuridica, il settore del digitale rischia di venire oltremodo compresso e non riuscire più a espandere le sue potenzialità a beneficio di una crescita economica, occupazionale e sociale degli stati e dei loro cittadini. È quanto avvertito negli Usa, dove vi è una preoccupazione che un approccio normativo eccessivamente precauzionale possa inibire lo sviluppo della AI, con implicazioni e penalizzazioni economiche, di sicurezza nazionale e geopolitiche²⁹. Uno dei più rilevanti interventi in tal senso è l'*Executive Order* 13859 del febbraio 2019, emanato dall'ex Presidente Trump, nel quale viene prospettata una strategia denominata *American AI Initiative*, che mira al raggiungimento dei seguenti obiettivi: promozione degli investimenti in ricerca e sviluppo nel settore della AI, da realizzarsi insieme a industria, università e *partner* internazionali; miglioramento nell'accesso ai dati; mantenimento della sicurezza da attacchi informatici; creazione dei presupposti per la crescita di una nuova generazione di ricercatori e utenti; mantenimento del vantaggio degli Usa nel settore e la protezione delle tecnologie di sicurezza nazionale più critiche dai *competitors* strategici e dagli avversari stranieri. Resta da vedere, però, se tale scenario rimarrà immutato o subirà dei cambiamenti con la nuova presidenza Biden.

Certo, non nego che ci sia bisogno di una regolazione del settore per evitare una sorta di anarchia giuridica, ma l'intervento normativo andrebbe fatto secondo principi generali e non norme di dettaglio. Se non altro per non incorrere nel rischio di normare fattispecie puntuali e circoscritte che saranno, a breve, superate dalla naturale evoluzione del fenomeno tecnologico. Che cambia, si trasforma e si sviluppa rapidamente: per fare solo un esempio, ieri erano i cellulari, oggi sono gli *smartphone* e domani chissà? C'è poi, ultimo ma non per ultimo, il motivo dello sviluppo della ricerca scientifica rivolta a migliorare la salute dei cittadini e più in generale il loro benessere di vita attraverso l'uso della AI, con le sue enormi potenzialità per diagnosticare e curare le malattie, per consentire di assumere, a tutti i livelli,

²⁶ Su cui, v. ora l'analitico commento V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

²⁷ Sulla cui proposta di regolamento, v. ora C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Riviste di BioDiritto*, 3, 2021. A questo proposito, si veda anche in questo fascicolo B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*.

²⁸ Su cui, v. O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet*, Oxford, 2021.

²⁹ Cfr. M.U. Scherer, *Regulating Artificial Intelligence System: Risks, Challenges, Competences and Strategy*, in *Harvard Journal of Law & Technology*, 29, 2016.

decisioni imparziali, per guidare le scelte dell'uomo attraverso l'uso degli algoritmi. Una legislazione fatta di principi generali avrebbe altresì il compito, più difficile ma più consono, di provare a disegnare il nuovo modello di società digitale, in cui la componente umana e quella artificiale verrebbero a essere chiamate a convivere in modo sostenibile, secondo un rinnovato principio di sussidiarietà, dove l'uno non dovrebbe prevalere sull'altro. L'umano ha creato l'artificiale con lo scopo di essere aiutato a creare le migliori condizioni per vivere meglio, in una società che sia sempre più libera e giusta.

4. Privacy, AI e GDPR nello spazio giuridico europeo

Torno sul tema della *privacy* e la sua trasformazione nell'era della AI.³⁰ Ormai, piaccia oppure no, punto di partenza obbligato è il Regolamento GDPR: da questa normativa occorre muovere per capire come la *privacy* e la sua tutela giuridica si intreccia con fatti e norme regolative delle nuove frontiere del digitale. Si possono evidenziare, sia pure riassuntivamente, quelle che sono le regole derivanti dal GDPR: ampliamento dell'ambito di applicazione territoriale; requisiti avanzati di inventario dei dati; aggravamento delle pene; nomina di un responsabile della protezione dei dati; obblighi più diffusi per i responsabili del trattamento dei dati; segnalazione di violazione dei dati personali più tempestiva; il diritto alla portabilità dei dati; il diritto all'oblio; maggiore consenso dell'interessato³¹. Una filiera di regole pensate per regolare le grandi aziende del *web* e i loro comportamenti per prevenire possibili violazioni della *privacy* delle persone, attraverso un uso disinvolto nel trattamento dei dati posseduti e archiviati. Salvo che i cd. giganti globali dell'informazione *online* padroneggiano il complesso ambiente normativo, che invece penalizza le piccole aziende indigene schiacciate dal peso della burocrazia imposta dal GDPR. Come è stato scritto: «Se lo guardiamo in modo oggettivo, il GDPR, di cui molti sostenitori europei della protezione dei dati sono così orgogliosi, sta facilitando il potere dei giganti digitali. E dietro le porte chiuse della Silicon Valley e della Cina spesso si sente dire: non è strano che gli europei non si accorgano nemmeno di come si stiano dando la zappa sui piedi?»³².

La critica nei riguardi del GDPR la si può muovere già fin dal suo primo articolo, secondo il quale «il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati». Quindi, la tutela della riservatezza quale diritto della personalità, deve

³⁰ Su cui, da ultimo, le riflessioni di G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021, 71 ss.

³¹ V. la sintesi del GDPR in E. Terioli, *Privacy e protezione dei dati personali Ue vs. Usa*, cit., 52 ss.

³² T. Ramge, V. Mayer-Schönberger, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, cit., 9.

coniugarsi con l'esigenza della libera circolazione dei dati: emerge un chiaro contrasto fra l'esclusività dei diritti assoluti indisponibili e la loro funzione circolatoria. Altre criticità possono essere evidenziate sia pure con alcuni lampi di luce che schiariscono parte del panorama legislativo europeo in punto di *privacy*. Peraltro, lo stesso Regolamento GDPR si applica anche alla AI, posto che questa è basata su dati personali e informazioni³³. Alla luce della proposta di regolamento UE sulla AI emergono alcuni problemi: innanzitutto, i dati personali (art. 4, n. 1, GDPR), ovvero di persona identificata o identificabile, e quelli anonimi, di cui fa largo uso la AI, i quali, laddove non classificabili, non possono, pertanto, essere soggetti alla normativa GDPR, creando così un vuoto regolativo. Poi, la qualità dei dati, che – secondo norma del Regolamento – devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; esatti e, se necessario, aggiornati» (art. 5, n. 1, GDPR). Si tratta di un'operazione più complessa da farsi nell'ambito dei sistemi AI, che seguono il criterio *garbage in, garbage out*. Ancora, il mancato ed esplicito divieto, da parte del GDPR, delle decisioni automatizzate ma piuttosto della limitazione dell'assunzione di decisioni prodotte unicamente con decisioni automatizzate. Mentre il sistema della AI sviluppa decisioni automatizzate sulla base degli algoritmi; anzi, uno degli aspetti di maggiore rilievo della AI consiste nel sapere giungere a una decisione automatizzata, salvo poi verificare se l'uomo vorrà assumerla oppure rigettarla, sia pure chiarendo e motivando l'utilizzazione dei dati e dell'algoritmo, con riferimento al suo scopo, ai suoi risultati e ai suoi potenziali pericoli³⁴. Infine, il problema della responsabilità civile e penale dei sistemi automatizzati³⁵: è il caso, più volte evocato, delle *driveless cars* e più in generale delle scelte di autonomia operativa in situazioni eticamente complesse, come quello dei *robot* chirurgici, dove, a oggi, l'uomo decide in modo competente se approvare o no una delle strategie generate dal *robot*. Ma che succede se i dati impiegati per imparare a generare strategie di intervento chirurgico riguardassero le strategie generate dai *robot* stessi e i corrispondenti esiti clinici?³⁶

Insomma, sembra quasi che il GDPR finisca col mettere vino vecchio in otri nuovi. È ancora una volta torna il tema già rappresentato nelle pagine precedenti: ovvero l'adeguamento della normativa alla luce dei continui e significativi cambiamenti di scenari giuridici dovuti al progresso tecnologico. Pertanto, si condivide l'opinione di chi ritiene che il GDPR non appare adeguato a disciplinare le applicazioni di AI. Perché «la logica del

³³ V. le osservazioni di G. Finocchiaro, *XVIII lezione: intelligenza artificiale, privacy e data protection*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, 331 ss.

³⁴ Discute anche questo problema, suggerendo l'assunzione del principio di “non discriminazione algoritmica”, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 196 ss.

³⁵ V. U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018.

³⁶ Problema discusso, tra l'altro, nel vol. F. Pasquale, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, tr.it., Roma, 2021.

Regolamento, basata sul consenso dell'interessato con riguardo ad uno specifico trattamento, non appare compatibile con i modelli attuali di gestione dei flussi di dati»³⁷.

In conclusione, si vuole lanciare una provocazione: e se fosse la AI a regolare la *privacy*? Ovvero, si può immaginare che sulla base dei *big data* si possa elaborare un algoritmo in grado di individuare le violazioni della *privacy*, specialmente quella che merita maggiore attenzione e preoccupazione: i cd. dati sensibili, che si riferiscono alle situazioni intimistiche dell'uomo, quali lo stato di salute, le scelte sessuali, religiose e politiche. Basterebbe che ogni qualvolta l'algoritmo individui un dato sensibile trattato senza il consenso dell'interessato, attivi un'azione preventiva di blocco del procedimento ovvero un'azione successiva con la prescrizione di una sanzione per la violazione di legge. Una provocazione, l'ho voluta definire. Eppure, la AI non è fantascienza: fa parte già delle nostre vite e lo sarà sempre più nell'immediato futuro.

Tommaso Edoardo Frosini
Dipartimento Scienze giuridiche
Università Suor Orsola Benincasa di Napoli
tommaso.frosini@unisob.na.it

³⁷ Così G. Finocchiaro, *XVIII lezione: intelligenza artificiale, privacy e data protection*, cit., 338.