Rivista Semestrale

Gennaio - Giugno 2022

N. 1/2022

Data Protection Law

Diritto delle nuove tecnologie, privacy e protezione dati personali

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it

Diretta da Elio Errichiello

DATA PROTECTION LAW – RIVISTA GIURIDICA

Rivista online non soggetta ad obbligo di registrazione ai sensi dell'art. 3-bis del Decreto Legge 103/2012

DIRETTORE:
Elio Errichiello

COMITATO SCIENTIFICO:
Elio Errichiello, Livia Aulino, Lucrezia D'Avenia, Rosanna Celella, Giulio Riccio.

Sito web: www.dataprotectionlaw.it

Contatti: info@dataprotectionlaw.it

"Data Protection Law" è una rivista elettronica di diritto Open access pubblicata dall'associazione Data Protection Law. La rivista pubblica con cadenza semestrale numeri costituiti da articoli scientifici inediti, saggi, traduzioni di estratti da opere scientifiche significative e di recente pubblicazione o articoli rilevanti per la comunità scientifica, recensioni di libri ed eventi culturali.
I numeri della rivista ospitano contributi scientifici prodotti e sottoposti su invito diretto della redazione.
Tutti i contributi sono sottoposti a doppia blind peer review.

Indice.

PIERO DE ROSA, Diritti e libertà in Internet: un mondo digitale è davvero sinonimo di libertà?

Pag. 3

TIZIANA DI PALMA, Il modello economico del lavoro digitale: i gig workers. riflessioni e analisi giurisprudenziale.

Pag. 15

SERGIO GUIDA, Gli algoritmi alla base di decisioni pubbliche fra intelligenza artificiale, tutela dei diritti e regole di buona amministrazione. Mediante la discrezionalità umana le features tecnologiche vanno temperate dai principi di ragionevolezza, trasparenza e motivazione.

Pag. 30

GUARINO GAETANO, Il caso Whatsapp contro l'autorità di vigilanza per la protezione dei dati personali in Irlanda.

Pag. 59

FRANCESCO LO CHIATTO, La Cybersecurity tra privacy e innovazione digitale.

Pag. 73

DIRITTI E LIBERTÀ IN INTERNET: UN MONDO DIGITALE È DAVVERO SINONIMO DI LIBERTÀ?

di Piero De Rosa

"A lot of people are on the Internet searching for fifteen minutes of fame. I've been on it so long and so often I'm looking for fifteen minutes of Freedom"

Stanley Victor Paskavich

SOMMARIO: 1. Concetto di libertà nella nuova frontiera digitale – 2. A quanta libertà siamo disposti a rinunciare per sfruttare i benefici delle nuove tecnologie? – 3. Conclusioni – Note bibliografiche.

Technological development represents a new opportunity for the promotion of human rights and digital freedoms, although, at the same time, it also creates new risks for these rights. Today, talking about virtuality – and specifically about Internet Freedom – means no longer taking into consideration the common territorial languages, but entering a new scenario in which the barriers of social distance fall and new bonds of belonging are created.
However, Internet Freedom is still limited, because it provides a skewed view of the relevance of human rights in the on-line environment.
The purpose of this paper, therefore, is to investigate the limits of digital freedom offered by new technological means and to ask ourselves how much freedom we are willing to give up in taking advantage of the benefits and processes of innovation, which induce radical transformations in our human existential dimension.

1. Concetto di libertà nella nuova frontiera digitale.

Le conquiste maturate negli ultimi anni nel settore delle tecnologie della comunicazione– e, in particolare, quelle registrate dall'inizio del nuovo millennio[1] – mettono in

[1] In linea generale, la comunicazione del nuovo millennio coinvolge un maggior numero di attori, l'integrazione di una ampia gamma di strumenti e l'introduzione di mezzi e tecnologie che accelerano e

luce gli effetti che stanno determinando nel tessuto economico, politico e sociale e conducono ad una riflessione sulle sfide alle libertà costituzionali tradizionali che, storicamente, hanno l'obiettivo di favorire la nascita di forme di democrazia sempre più diffuse ed evolute[2].

Partendo dalla considerazione del dato storico è evidente come la vita contemporanea risulti caratterizzata dal peso crescente della tecnica che, grazie ai ritmi di una innovazione sempre più accelerata, ha portato ad una radicale trasformazione e ad una espansione progressiva delle antiche libertà costituzionali mai registrate in precedenza[3].

Tale evoluzione riguarda generalmente tutti i settori ma colpisce, in maniera particolare, proprio il campo della comunicazione che riflette maggiormente l'evoluzione della tecnologia, dell'economia e della vita sociale[4]. Ancora maggiore, infatti, è l'esigenza di riflettere sulla istituzione espressiva del concetto di "comunicazione" che, nel nuovo scorcio di secolo, ha visto l'esplosione su scala mondiale di strumenti tecnologico-informatici in grado di rendere le comunicazioni multimediali, ossia capaci di coinvolgere nel proprio processo i diversi sensi umani, istantanee ed incuranti delle distanze.

Dal 1981, quando il *personal computer* è apparso sul mercato dei beni di massa, si è imposto un nuovo metodo di elaborazione, di trasmissione e di stoccaggio delle conoscenze e delle informazioni e, proprio il settore della comunicazione, transitando dall'analogico al digitale, ha accresciuto notevolmente la sua importanza[5].

---

aggiornano continuamente azioni e procedure. Cfr. C. BANDIERA, L. MAROZZI, *Comunicare nel 2000. Tendenze della comunicazione alle soglie del nuovo millennio*, Franco Angeli Editore, 1999.

[2] Per una analisi più approfondita dell'impatto delle nuove tecnologie sulla società e i diritti fondamentali, si veda T. E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier Università, 2017.

[3] Dal punto di vista costituzionale si può constatare come Internet abbia esteso i tradizionali diritti: dalla libertà di espressione o di riunione e associazione, al diritto alla salute, all'iniziativa economica privata, al lavoro, allo studio, ai diritti politici e molti altri ancora. Internet estende la portata dell'art. 21 Cost. perché permette a tutti ed a costi bassissimi di esprimere il proprio pensiero non solo con riferimento al titolare del diritto («tutti hanno il diritto…») e l'oggetto del pensiero («di manifestare liberamente il proprio pensiero…») ma anche con riferimento alle modalità e soprattutto all'accesso al mezzo. Sul punto, cfr. G. D'IPPOLITO, *La libertà informatica e il diritto di accesso ad Internet*, 2014.

[4] Storicamente la comunicazione si è sviluppata e si è affermata progressivamente nell'impiegare strumenti sempre più "sofisticati" e nell'investire sulle capacità delle strategie comunicative dei soggetti interagenti. Le informazioni hanno, in tal modo, cominciato a circolare ad una maggiore velocità e ad un costo meno elevato.

[5] Cfr. G. DE MINICO, *Antiche libertà e nuova frontiera digitale*, Giappichelli Editore, 2016.

Nella società elettronica, infatti, l'avvento dei *mass media* interattivi ha rappresentato non soltanto l'elemento unificatore dei diversi mondi della comunicazione, ma ha anche trasformato dalle radici i canoni delle comunicazioni di massa precedenti e le vie che stanno portando, a livello planetario, al loro progressivo sviluppo.

A riguardo, Nicholas Negroponte, fondatore e presidente emerito del *Media Lab* del *Massachusetts Institute of Technology (MIT)*, ha affermato che nel campo delle comunicazioni della nostra civiltà:

"There is no speed limit on the electronic highway."[6]

La possibilità non soltanto di raccogliere informazioni e dati, ma anche di diffonderli è, probabilmente, il primo e più visibile effetto dell'ingresso di Internet nella quotidianità di strati sempre maggiori di popolazione[7].

È questo il periodo in cui si concretizzano tutti i presupposti tecnologici indispensabili per lo sviluppo di una comunicazione sempre più interattiva che ha rivoluzionato profondamente il sistema di comunicazione offerto dai *mass media* tradizionali. Da qui l'importanza di quella "tecnologia sociale" costituita dal diritto stesso, intesa sia come riconfigurazione del regime dei diritti tradizionali, sia come invenzione di diritti "nuovi".

Nello stesso tempo, l'interazione tra televisione, *personal computer* e satellite ha condotto ad una globalizzazione di tutto ciò che viene prodotto e della sua distribuzione, facendo confluire il tutto nell'unico universo dell'industria dell'informazione[8].

Da qui la nascita di una cosiddetta *"società dell'informazione"* caratterizzata da un incremento dei consumi di comunicazione e del tempo sociale ad essi dedicato, neutrale rispetto ai contenuti trasmessi e che ha condotto, mediante il processo di digitalizzazione, ad una convergenza delle reti informatiche, di telecomunicazione e radiotelevisive.

---

[6] Cfr. N. NEGROPONTE, *Being Digital*, 2015.

[7] Cfr. C. MELZI D'ERIL, G. E. VIGEVANI, *Lo statuto dell'informazione su Internet,* in (a cura di) T. E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), Diritti e libertà in Internet, Le Monnier Università, 2017.

[8] La Rete sta assumendo un ruolo di crescente importanza anche come canale di sfruttamento di film e serie TV, grazie all'affermarsi di servizi come *Netflix*, *Amazon Prime Video* e *iTunes*.

A ciò aggiungasi che sulla Rete la comunicazione interpersonale e le interazioni sociali tra le persone assumono caratteristiche innovative e peculiari e con tratti del tutto differenti rispetto a quelli dei precedenti mezzi di comunicazione[9]. La particolare caratteristica della comunicazione via *computer*, infatti, rende più facile il flusso dell'informazione consentendo a chiunque, nei limiti del possibile, di partecipare alla creazione di nuovi contenuti informativi, di conoscenza e di intrattenimento[10].

Ne consegue che lo sviluppo della personalità di un individuo (e la sua soddisfazione) si stratificano nell'ecosistema digitale e alimentano lo stesso concetto di "diversità", inteso come ampia diffusione dell'informazione da parte di una grande varietà delle fonti e come fondamentale strumento per garantire e tutelare le procedure di decisione democratica[11].

Prendendo ad oggetto proprio la libertà di manifestazione del pensiero – che, insieme alla libertà personale, ha rappresentato la pietra angolare del costituzionalismo moderno – risulta evidente l'inadeguatezza delle formulazioni dei diritti fondamentali contenute nelle Carte del Novecento rispetto allo sviluppo delle nuove tecnologie.

Soprattutto per quanto concerne i diritti di ultima generazione, l'uso virtuoso delle tecnologie impegna ormai non più semplicemente i soli individui o i singoli ordinamenti, dal momento che il godimento – o, al contrario, la compromissione – delle libertà tende ormai ad assumere rilevanza a livello sovranazionale (se non, addirittura, globale).

Da quando si è affermata la realtà del *web*, da parte dei giuristi e degli esperti del settore, si è registrato uno sforzo e un tentativo continuo di allargare il riconoscimento dei diritti fondamentali tradizionali agli aspetti specifici delle nuove tecnologie e di individuare un catalogo di diritti digitali *in* Internet e *per* Internet, intesi come diritti legati esclusivamente all'utilizzo della Rete.

Tra gli addetti ai lavori prevale, tuttavia, il timore che una eccessiva regolazione di Internet possa restringere e limitare le illimitate libertà e le opportunità offerte dalla

---

[9] Cfr. L. PACCAGNELLA, *La comunicazione al computer*, Il Mulino, 2000.

[10] Cfr. U. GASSER, *The Good, the Bad and the Ugly: An essay on Information Quality Governance on the Internet*, 2008.

[11] Per poter prendere buone decisioni, ci affidiamo all'informazione di qualità, ovvero a quella informazione che soddisfa le esigenze funzionali, cognitive ed estetiche dei diversi titolari di interessi quali gli utenti, i creatori, gli esperti e gli amministratori. Ne consegue che i sistemi di diritto e regolamentazione normativa dovrebbero contribuire alla creazione e allo sviluppo ulteriore di un ecosistema di informazione di elevata qualità. Sul punto, cfr. G. ZICCARDI, *Nuove tecnologie e diritti di libertà nelle teorie nordamericane*, Enrico Mucchi Editore, 2007.

Rete, violando quella *net neutrality* che dovrebbe, al contrario, connotarla come strumento di crescita sociale e culturale.

Conseguentemente, il nocciolo duro della regolamentazione giuridica del *web* ruota intorno ad un c.d. "diritto di accesso", vale a dire di uso e di disponibilità della Rete e dei suoi servizi e sofferma la riflessione sulla libertà di utilizzo e di assenza di ogni controllo, sia di tipo pubblico che privato[12].

Pertanto, la funzione primaria del diritto rimane fondamentalmente quella di orientare il processo di trasformazione indotto dal progresso tecnologico verso l'affermazione di interessi comuni fondati sui valori costituzionali della solidarietà e dell'uguaglianza, non meramente orientati sulla tutela di interessi privati in base alla forza capitalistica dei mercati.

Da qui l'esigenza di adottare politiche costituzionali e regole giuridiche in grado di limitare e indirizzare le multinazionali del *web* verso obiettivi di interesse quasi pubblico allo scopo di proteggere la società dai rischi insiti nell'utilizzo stesso delle nuove tecnologie, ragionando in termini di solenni dichiarazioni o di costituzioni per il c.d. *cyberspazio*.

Non è un caso che la Dichiarazione dei diritti in Internet, licenziata il 14 luglio 2016 dalla Commissione speciale per i diritti e doveri relativi a Internet, nel suo preambolo afferma che:

"Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet deve essere considerata come una risorsa globale e che risponde al criterio della universalità."[13]

[12] Si pensi all'*Internet Bill of Rights* o anche al c.d. diritto di *habeas data* riproposti a livello internazionale.

[13] Cfr. https://www.generazioniconnesse.it/_file/documenti/Dichiarazione_diritti_Internet_2016/Boldrini.pdf

Al di là della forza giuridica o meno della Dichiarazione[14], vi è il tentativo di porre l'attenzione sulla dimensione di Internet dove, accanto a nuove opportunità per l'esercizio dei diritti umani, si manifestano anche forme inedite di minaccia.

La Rete, per sua natura, è configurata come uno spazio pubblico, sganciato dalla sfera della sovranità nazionale, ovvero come un "bene comune" che dovrebbe restare sottratto alla disponibilità del potere privato e attraverso il quale si realizzano le nuove forme di partecipazione individuale e collettiva alla vita democratica[15]. Tuttavia, questa impostazione muove dall'idea di fondo che Internet e il suo mondo siano una realtà diversa e separata da quella reale, una libera *agorà* in cui è necessario presidiare le libertà insite nel suo utilizzo[16] quando, tuttavia, la Rete risulta essere già parte integrante del nostro mondo fisico.

L'utente diventa così *"cittadino di Internet"* e, grazie alle opportunità offerte dalla Rete, massimizza e amplia le sue libertà fondamentali, sviluppando appieno la sua personalità sia come singolo sia nelle modalità associative che essa consente e compiendo appieno il dettato di cui all'art. 2 della Costituzione. In effetti, la verifica circa l'identificabilità di Internet come spazio di "formazione sociale" conduce alla considerazione che la "comunità elettronica"[17] possa integrare in larga parte i requisiti minimi necessari perché possa parlarsi di formazione sociale[18].

---

[14] Vedi, sul punto, cfr. M. BASSINI, O. POLLICINO, *Verso un Internet Bill of Rights*, Aracne Editrice, 2015.

[15] Si pensi, a titolo esemplificativo, alla *"Dichiarazione di Indipendenza del Cyberspazio"* in cui, in toni apocalittici, veniva affermato sostanzialmente che i governi nazionali non avevano alcuna sovranità nel nuovo spazio digitale. La Dichiarazione è consultabile al seguente link: https://www.eff.org/it/cyberspace-independence

[16] Il diritto di accesso ad Internet è un diritto fondamentale che favorisce l'esercizio di altri diritti fondamentali, dalla libertà di espressione al diritto di informare ed essere informati, alla libertà di impresa e di innovazione, alla libertà di associazione. Nel *cyberspazio* la premessa indispensabile per l'effettivo esercizio di queste libertà è la neutralità della Rete. Cfr. A. MASERA, G. SCORZA, *Internet. I nostri diritti*, Editori Laterza, 2016.

[17] Cfr. P. MARSOCCI, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare*, 2015.

[18] Al fine di qualificare le formazioni sociali in "senso forte", cioè come veicolo del pluralismo sociale che informa il nostro ordinamento, sono presi in considerazione tre elementi fondamentali: l'*elemento materiale*, dato dalla riferibilità del termine ad un insieme di soggetti persone fisiche, l'*elemento tecnologico*, rappresentato dallo scopo di tali aggregazioni di contribuire, seppure in modo non primario, allo sviluppo della persona umana, e, infine, *all'elemento psicologico* interno ai componenti della formazione sociale consistente nella coscienza o volontarietà di farne parte e perseguire gli scopi che essa si propone. Sul punto, cfr. E. ROSSI, *Le formazioni sociali nella Costituzione italiana*, Cedam, 1989.

Peraltro, il proliferare delle piattaforme digitali, i c.d. *"social network"*, ha radicalmente modificato il nostro modo di comunicare, consentendo una condivisione immediata di un numero illimitato di informazioni e ponendo sempre più frequentemente i legislatori di tutti i Paesi di fronte a questioni e problematiche non sempre di semplice soluzione[19].

La tendenza delle strutture della Rete è quella, appunto, di incoraggiare la condivisione di informazioni: senza informazioni la Rete non sarebbe né viva, né sociale.

Mentre l'ideologia di Internet ne enfatizza la natura decentralizzata, la *"cultura della piattaforma"* ha portato gli utenti a trovare la loro dimora comune nelle piattaforme partecipative in Rete quale luogo di sintesi della interazione e della integrazione di soggetti diversi tramite una varietà di applicazioni, con il risultato che gli utenti si trovano rinchiusi in "giardini" recitanti e centralizzati[20].

I *social network* offrono l'occasione di un costante e silenzioso monitoraggio delle attività, dei consumi e dello "stare in contatto", naturalizzando, istituzionalizzando e mediatizzando la sorveglianza reciproca, spingendo gli utenti stesso verso un mondo che appare ristretto e gestito da algoritmi su cui non hanno alcun tipo di controllo[21].

La visione delle pratiche altrui realizzata sui principali *social network* rappresenta così una modalità privilegiata per comprendere cosa fanno e come sono gli altri, in un continuo processo di sguardo reciproco, alimentando un controllo delle masse sempre più invasivo e molto più efficace rispetto alle dittature del passato, divenendo uno strumento di *marketing* e di politica, un mercato di pubblicità, un luogo di raccolta delle informazioni private (allo scopo di rivenderle) e un *business* miliardario per chi ha il controllo su tali strumenti[22].

---

[19] Oggi l'utilizzo di Internet e degli *smartphone* è dominato dai *social media*: la diffusione di applicazioni e servizi da utente a utente basati sul *web* alimenta una esplosione di dialoghi informali e contenuti generati dagli utenti dando vigore ad una "cultura partecipativa" sempre più massiva.

[20] Cfr. G. LOVINK, *L'abisso dei social media. Nuove reti oltre l'economia dei like*, Egea Editore, 2016.

[21] Essendo il risultato di un procedimento automatico, l'algoritmo è contenuto in una "scatola nera" (o *black box*) i cui meccanismi di calcolo non sono predefiniti, e possono essere complicati fino al punto da divenire incomprensibili. Si veda, a riguardo, cfr. F. DELLA PORTA, *Una breve storia della globalizzazione*, Ronzani Editore, 2021.

[22] Cfr. F. GALGANI, G. RIPA, *L'era della simulazione ovvero l'oscuro desiderio di essere sempre connessi. Pericoli potenziali e reali che la "connessione virtuale" porta con sé*, 2016.

Stare in contatto, essere aggiornati, ricevere informazioni e comunicazione dalla rete personale sono le principali motivazioni all'uso dei *social network*, mostrando di essere il denominatore che accomuna la maggioranza degli utenti al loro frenetico utilizzo.
Sorge così spontanea la riflessione su cosa si debba intendere veramente per libertà nella nuova era della tecnocrazia.

2. A quanta libertà siamo disposti a rinunciare per sfruttare i benefici delle nuove tecnologie?

Come già può essere risultato chiaro dalle considerazioni fin qui esposte, soprattutto per quanto riguarda la nuova dimensione esistenziale consentita dal rafforzamento delle libertà legate alla trasmissione del pensiero, emerge la necessità di ragionare sull'impatto delle tecnologie sulla fisionomia delle libertà fondamentali tradizionali.
La capacità connettiva della Rete, infatti, offre a strati sempre più ampi della popolazione mondiale la straordinaria possibilità di un accesso agevole e immediato ad un sistema di scambi informativi in tempo reale. Ad oggi, tale sistema interattivo ha rappresentato la condizione indispensabile per la produzione culturale nei vari ambiti del sapere e ha assunto un ruolo centrale nel flusso di informazioni.
Tuttavia, è doveroso muovere dalla constatazione di come il progresso tecnologico contiene in sé una strutturale ambivalenza in quanto può recare, accanto ad indubbi benefici materiali e spirituali, anche nuove minacce per la vita e la libertà individuale, richiamando l'attenzione dei giuristi (e degli altri addetti ai lavori) sulla necessità di affermazione di un "principio di precauzione" e di "libertà responsabile" che deve guidare l'utilizzo delle nuove tecnologie[23].
Con l'avvento dei *Big Data* e di sempre più sofisticate tecnologie di analisi degli stessi, si pone la questione dei rischi ai quali ciascuno di noi, anche inconsapevolmente, si può esporre[24].
Oggi, il fenomeno tecnologico non è più solo, come in passato, una questione di *privacy*, ma nell'ottica dell'orizzonte giuridico offerto dalla Rete, c'è anche la *privacy*: la

[23] Cfr. A. SIMONCINI, *Sovranità e potere nell'era digitale,* in (a cura di) T. E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), Diritti e libertà in Internet, Le Monnier Università, 2017.
[24] A questa produzione primaria di dati, va aggiunta la crescente capacità delle macchine di imparare in maniera automatizzata dai dati stessi consentendo la loro trasformazione in informazioni su attitudini, interessi e propensioni degli utenti.

forza di accelerazione della tecnica e della scienza che caratterizza le molteplici interazioni con il mezzo tecnologico è all'origine di ansie e timori nel vedere violata la propria riservatezza di dati e di informazioni personali e sensibili[25], ma soprattutto sta facendo nascere nuovi e impellenti bisogni di normazione.

Il "paradigma tecnologico" che ha caratterizzato (e che ancora caratterizza) il XXI secolo concerne così la natura stessa della relazione tra l'uomo e la realtà che lo circonda, la sua capacità intellettiva e cognitiva e, di conseguenza, la sua attitudine relazionale a cui il fenomeno giuridico risulta strettamente correlato.

Il diritto, infatti, nasce dalle relazioni interpersonali e, di conseguenza, l'impatto della rivoluzione digitale riguarda proprio il problema di come l'umanità stia trasformando la propria visione del mondo e delle proprie libertà legandole sempre di più al fenomeno del progresso tecnologico[26].

L'associazione concettuale di Internet alle "formazioni sociali", richiamate dal dettato dell'art. 2 della Costituzione, comporta che, di fatto, la Rete è un nuovo luogo dove incontrarsi e scambiarsi informazioni sulla base dei propri interessi specifici e, conseguentemente, il riconoscimento di un generale diritto di accesso ad Internet diviene prerogativa indefettibile per l'esplicarsi delle libertà fondamentali.

Garantire l'accesso alla Rete, pertanto, costituisce lo scopo primario delle politiche nazionali e sovranazionali, anche al fine di colmare quel *digital divide* tra chi ha accesso (adeguato) ad Internet e chi non ce l'ha (per scelta o no), le carenze culturali digitali e le disuguaglianze tra gli individui e le popolazioni a cui ancora è negata la disponibilità delle tecnologie di base.

Peraltro, l'eventualità di riconoscere un fascio di diritti del tutto consustanziali alla Rete ad una *élite* ristretta di inclusi – intesa come rete di soggetti istruiti e competenti nel processo tecnologico – non potrà che portare al rischio di una *"technoapartheid"* all'interno di una comunità sempre più interconnessa e globalizzata. Basti pensare che proprio Internet si caratterizza per la sua naturale vocazione all'extraterritorialità, in quanto esso travalica i confini nazionali ed elimina le differenze culturali fra i popoli[27].

Appare evidente, allora, come ogni settore dell'esperienza umana è stato rapidamente trasformato dal progresso e dalla diffusione delle nuove tecnologie che sono diventate

[25] Si pensi, a titolo esemplificativo, al cyberbullismo o al *sexting*, al *deep faking* e alle *fake news*.

[26] Sul punto, A. SIMONCINI, *Sovranità e potere nell'era digitale,* in (a cura di) T. E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), Diritti e libertà in Internet, Le Monnier Università, 2017.

[27] Cfr. T. E. FROSINI, *Il diritto di accesso a Internet*, (a cura di) T. E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), Diritti e libertà in Internet, Le Monnier Università, 2017.

il primo e più efficace motore di cambiamento sociale, lavorativo e culturale della nostra epoca.

Ogni cambiamento epocale e antropologico comporta indubbiamente una serie di aspetti problematici, proprio in virtù della complessità delle trasformazioni in corso, della crescente rapidità con la quale esse si vengono a realizzare e della inadeguatezza delle leggi attuali a regolamentarne il forte impatto sulla società[28].

La difficoltà a comprendere la natura di Internet e la serie complessa di possibilità offerte, rischia di complicarsi ulteriormente se si considera che l'impiego della Rete tende ad alterare il comportamento e il funzionamento della mente, in modo tale da creare nuovi modelli di interazione con il reale e di alterazione della dimensione emotiva e affettiva[29].

La tecnologia digitale è, ormai, onnipresente e caratterizza le nostre vite: basti pensare agli *smartphone* o ai *tablet* che abbiamo sempre a portata di mano in ogni momento della giornata.

L'utilizzo eccessivo delle tecnologie porta così l'individuo, sempre più spesso, a dissociarsi dalla realtà e a vivere, in casi estremi, in uno stato di vera e propria alienazione, aumentando il rischio di appiattimento, di omologazione, di frammentazione, di individualismo, di superficialità nell'accesso alle conoscenze e nella sperimentazione di nuove relazioni sociali[30].

Alcuni soggetti possono sviluppare una vera e propria dipendenza da *social network*, dimenticandosi di vivere in collettività effettive[31] e il malfunzionamento, seppure per poche ore, delle piattaforme partecipative in Rete che, tengono ogni giorno in contatto miliardi di persone, fa nascere la sensazione di essere *off-line*, fuori da quel mondo digitale che è diventato abitudine.

---

[28] Cfr. K. SCHWAB, *Governare la quarta rivoluzione industriale*, Franco Angeli Edizioni, 2019.

[29] Cfr. G. CAVIGLIA, R. PERRELLA, *Dipendenza da Internet*, 2014.

[30] Sul punto, cfr. C. MAZZUCCHELLI, *La solitudine del social networker*, Delos Digital, 2014.

[31] Come afferma lo psichiatra Manfred Sptizer, "demenza non significa soltanto mancanza di memoria e, nel caso della demenza digitale non si tratta solo del fatto che soprattutto tra i giovani questa caratteristica sembra sempre più diffusa […]; il problema riguarda soprattutto il rendimento mentale, il pensiero, la capacità critica e di orientarsi nella giungla delle informazioni", cfr. M. SPITZER, *Demenza Digitale*, Corbaccio Editore, 2014.

In una sorta di profezia orwelliana[32] vi è un monito: ai nostri giorni, dopo la Rivoluzione digitale, l'umanità si trova a fronteggiare le insidie e i pericoli delle nuove tecnologie, che hanno una capacità inimmaginabile di sorveglianza sui cittadini. Conseguentemente, in questo scenario, hanno acquisito un ruolo di primo piano i gestori dei servizi di connettività che "danno accesso a, ospitano, trasmettono e indicizzano contenuti originati da terze parti o forniscono servizi basati su Internet a terze parti"[33].
Emerge allora la necessità interrogarsi sulle cause che hanno spinto l'uomo dell'era post-industriale ad abdicare sostanzialmente alla sua originaria idea di libertà e domandarsi se i cittadini abbiano inconsciamente accettato la loro sudditanza alle nuove Intelligenze Artificiali.
In questo rapporto sovvertito tra uomo e tecnologia si è assistito all'affermarsi di un gigantismo della tecnica e dell'informatica e alla loro massima diffusione, alimentando, al contempo, un calo di tensione del pensiero comune e uno scarso interesse per la libertà, come se essa costituisca una prerogativa della società moderna e come tale non possa mai perdersi.
Pertanto, al fine di opporre una diga al dilagare sempre più avvertito e condiviso di queste percezioni, appare fondamentale sviluppare una riflessione critica sulla tecnologia e sui suoi effetti reali nella vita di tutti i giorni, partire cioè da una vera e propria "tecnoconsapevolezza"[34] sulla nuova dimensione sociale dell'individuo/utente nell'era di Internet. Alfabetizzarci digitalmente, capire come funziona il *web*, chi lo controlla e come utilizzarlo.
Rimanendo in attesa di un intervento incisivo del legislatore che, in maniera consapevole, metta mano alla materia, non bisogna tuttavia ignorare che la Rete resta un luogo dove i diritti, i doveri e le responsabilità trovano un loro spazio e una loro dignità e in cui dovranno continuare ad essere applicati i principi di civiltà giuridica affermati nelle Carte dei diritti del secondo dopoguerra.

---

[32] Innumerevoli soni i punti di contatto tra il mondo di "1984" in cui si descrive una società dominata dal "Grande fratello" e quello odierno, in cui i dati personali sono diventati merce preziosa. Il dittatore cui si fa riferimento nel libro è un uomo misterioso, che nessuno ha mai visto in faccia, ma che conosce tutto di tutti, perché controlla costantemente la vita di ogni cittadino.
[33] OECD, 2010, https://www.oecd.org/digital/ieconomy/44949023.pdf
[34] Cfr. C. MAZZUCCHELLI, *La tecnologia non è il male, ma riflettere sui suoi effetti è urgente: ecco perché*, 2019.

3. Conclusioni.

Venendo al dunque, non c'è dubbio che l'impatto della tecnologia sulle situazioni soggettive abbia, almeno nella sua fase genetica, aperto nuovi spazi di libertà di cui hanno goduto anche i diritti tradizionali sotto la lente d'ingrandimento dell'innovazione digitale.

La rivoluzione apportata da tale fenomeno – non registratosi in precedenza per gli altri *mass media* – riflette il ruolo e il valore che ormai Internet ha acquisito a livello globale nel conformare i diritti e gli interessi delle persone, sia come singole che all'interno di una comunità sempre più digitale e interconnessa.

Lo studio del diritto degli intermediari apre, dunque, ad una nuova riflessione su come le attività degli stessi intermediari incidano effettivamente sugli interessi giuridicamente rilevanti e su come le diverse regolamentazioni nazionali o sovranazionali possano contribuire a favorire o ad ostacolare il godimento delle libertà fondamentali.

Resta il fatto che i nuovi mezzi tecnologici introducono una variazione importante: il virtuale.

È proprio sul terreno meno solido delle tecnologie – e nella distinzione tra reale e virtuale – che il diritto è chiamato a stabilire quali usi ed obiettivi vadano considerati antigiuridici all'interno di un sistema che è stato costruito e basato sui valori liberal-democratici.

Il problema di fondo risiede, dunque, nell'utilizzo che si fa della Rete non inteso semplicemente come mezzo tecnologico in generale, ma inserito all'interno di un sistema di tipo capitalistico che ha come obiettivi principali il profitto e il controllo delle masse da parte dei grandi giganti del *web*.

Si richiamano allora le parole di Joseph Weizenbaum, informatico tedesco, autodefinitosi dissidente ed eretico dell'informatica, secondo il quale è necessaria una maggiore capacità di indagine e pensiero critico nell'approcciarsi ai nuovi mezzi tecnologici:

"Per una comprensione critica dobbiamo prima fermarci ad ascoltare, non limitandoci a sentire, ma imparando a interpretare e a comprendere."[35]

[35] Cfr. J. WEIZENBAUM, *Computer Power and Human Reason: From Judgment to Calculation*, 1976.

L'invito a fondare una critica della Rete non è una mera posizione aliena o da *"outsider"*, ma una riflessione sulle nuove dimensioni esistenziali consentite dal rafforzamento delle libertà legate alla trasmissione stessa del pensiero per mezzo dei nuovi progressi tecnologici.

Infatti, soltanto con una maggiore consapevolezza possiamo rendere le tecnologie di controllo del *web* un vero strumento di crescita e di progresso, contribuendo non soltanto una riconfigurazione del regime dei diritti tradizionali, ma anche alla creazione di diritti nuovi *in* Internet e *per* Internet.

Note bibliografiche.

CARR N., *Is Google Making Us Stupid?*, 2008, https://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/306868/

FROSINI T. E., POLLICINO O., APA E., BASSINI M. (a cura di), *Diritti e libertà in Internet*, Le Monnier Università, 2017.

LOVINK G., *L'abisso dei social media. Nuove reti oltre l'economia dei like*, Egea Editore, 2016.

LOVINK G., *Ossessioni collettive. Critica dei social media*, Egea Editore, 2012.

LOVINK G., *Internet non è il paradiso*, Apogeo Editore, 2004.

OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Giappichelli Editore, 2014.

RAMONET I., *Tutti sotto controllo*, 2014, Le Monde Diplomatique, http://www.ariannaeditrice.it/articolo.php?id_articolo=48062

ZICCARDI G., Nuove tecnologie e diritti di libertà nelle teorie nordamericane, Mucchi Editore, 2007.

IL MODELLO ECONOMICO DEL LAVORO DIGITALE: I GIG WORKERS. RIFLESSIONI E ANALISI GIURISPRUDENZIALE

di Tiziana Di Palma

SOMMARIO: 1. Gig-economy e lavoro on demand – 2. Dalla subordinazione all'etero-organizzazione. Analisi giurisprudenziale – 3. Il "ritorno" alla natura subordinata del rapporto di lavoro dei riders addetti al "food delivery".

The economic model of the so-called Gig economy has developed in recent years thanks to digital platforms that offer increasingly advanced personalized services, able to reach an increasingly large number of users. The clearest example of the Gig economy is represented by the food delivery sector. Recently, the Italian labor courts have been invested in disputes concerning the qualification of the work rendered by riders, workers of the food delivery sector.

1. Gig-economy e lavoro on demand

Il modello economico della cd. *Gig economy* ("*economia dei lavoretti*") si è largamente sviluppato negli ultimi anni grazie alle molteplici piattaforme digitali che offrono servizi personalizzati "*on demand*" sempre più avanzati, in grado di raggiungere un numero sempre più corposo di utenti.

Nel gennaio del 2009, il direttore del Daily Beast, Tina Brown annunciava l'avvento della *Gig economy,* definendola come l'insieme dei lavori temporanei, consulenze, prestazioni offerte come freelance in grado di garantire un reddito annuo dignitoso, consentendo il mantenimento di un terzo dei lavoratori americani, ovverosia il raggiungimento del "*pareggio di bilancio personale e familiare"* definito colloquialmente "*the Nut*"[36].

Hillary Clinton, già Segretaria di Stato U.S.A., nel 2015, dichiarò, poi, che "*nel frattempo, molti americani stanno facendo soldi extra affittando una piccola stanza, progettando siti web, vendendo prodotti da loro stessi progettati a casa o persino guidando la propria auto. Questa economia su domanda, la cosiddetta gig economy, sta*

[36] C. CUCCINELLO, LA REPUBBLICA, ECONOMIA & FINANZA, 19.10.2015.

creando stimolanti economie e scatenando l'innovazione. Ma sta anche sollevando domande difficili sulle protezioni lavorative e su come sarà un buon lavoro in futuro" (Howard, 2015)[37].

La Gig economy è da intendersi, dunque, quale nuovo modello di *matchmaking* tra domanda ed offerta di lavoro, ovverosia un "*modello di lavoro su richiesta, ove domanda ed offerta si incontrano on line attraverso apposite piattaforme digitali*", così come definito del XVII Rapporto dell'I.n.p.s. del luglio 2018, non più fondato su prestazioni lavorative continue e a tempo indeterminato, ma sul lavoro "*on demand*", ovverosia a richiesta, il che si combina, spesso, con esigenze di flessibilità e anche in forme di precarietà.

Si sostiene, invero, che, da una parte, ci sarebbe uno spostamento del rischio dall'impresa al lavoratore *("a radical shift of business risk away from platforms and onto individual workers*") e, dall'altro, un danno alla stessa innovazione tecnologica in ragione dell'utilizzo di lavoro a basso costo ("*the real danger that this recourse to cheap labour incentivises the very opposite of genuine innovation*")[38].

L'I.n.p.s. rileva come i problemi di definizione della gig economy si riflettano nella difficoltà di identificare i datori di lavoro e di lavoratori, non esistendo un codice Ateco che permetta di individuare le aziende né esiste una sola forma di pagamento, dovendosi ogni analisi ritenere parziale.

Il più chiaro esempio di *Gig economy* è rappresentato dal settore del *food delivery*, consistente nella consegna a domicilio di cibi e bevande ordinate da clienti di bar e/o ristoranti direttamente attraverso piattaforme digitali e che vengono consegnati ad opera dei *riders*, cioè fattorini che adoperano i propri veicoli (biciclette, motocicli) per il trasporto dei cibi ordinati.

L'idea del cd. *Food delivery* era nata nel 2001 con la danese *Just Eat*, con l'intento di aggregare le offerte di più ristoranti su di un'unica piattaforma digitale posta a disposizione del cliente. Tale modello fu superato da altre aziende come l'inglese *Deliveroo*, nel 2013, e la tedesca Foodora, nel 2014, che, oltre a gestire i rapporti con i ristoranti, si occupavano anche della logistica delle consegne.

[37] A. HOWARD, *It's time to talk about the gig economy*, in *The Huffington Post*, 14.07.2015.
[38] J. PRASSL, *Humans As Service*, Oxford, 2017.

Si premetta che il *platform work* racchiude al suo interno una pluralità di modelli di lavoro, non facilmente distinguibili data la sua natura complessa ma comprendenti, a grandi linee, il lavoro *on demand* tramite app, il *crowdwork*, *l'asset rental*.

Nel primo caso, talune attività di lavoro "tradizionali" – tra le quali la consegna di cibo a domicilio o al trasporto di passeggeri o, ancora, alle riparazioni di idraulica o altri lavori manuali da eseguire in casa – vengono svolte dal prestatore mediante l'intermediazione di un'applicazione digitale per *smartphone* che opera localmente (*Deliveroo, Handy, Wonolo, Uber, BeMyEye, Lyft, Care, Foodora* etc.).

Nel secondo caso (*crowdwork*), una piattaforma virtuale (si pensi ad Amazon Turk o Task Rabbit) consente l'assegnazione di una serie di compiti, spesso di carattere ripetitivo (come l'inserimento di dati o la compilazione di tabelle per Excel) e da svolgersi normalmente al PC da remoto, ad una persona selezionata all'interno di una serie indefinita dei potenziali individui candidatisi online.

Nell'*asset rental*, affitto e noleggio di beni e proprietà, la prestazione lavorativa è accessoria, come nel caso del proprietario di un appartamento concesso in fitto su AirBnb che cura anche l'accoglienza e le pulizie finali.

Secondo tale modello, la richiesta del cliente non riguarda una prestazione lavorativa, bensì la possibilità di utilizzare, pagando, un bene o una proprietà altrui, in genere, per un breve periodo, come nel caso di BlaBlaCar, ShareWood, AirBnb etc.

Per dare una dimensione quantitativa al fenomeno, ci si affida agli studi sostenuti da organizzazioni internazionali, da Università e da società di consulenza (Eurofund per l'Europa e Cornell University per gli Stati Uniti)[39] da cui emerge che, negli U.S.A., a fine 2015, circa lo 0,15% degli occupati fosse impiegato in attività di gig economy; nel 2016, includendo oltre agli U.S.A. anche i Paesi UE-15, una ricerca del McKinsey Global Institute stima che la quota di *indipendent workers* sia il 20-30% della popolazione in età lavorativa, di cui circa il 15% ha lavorato per piattaforme digitali[40]; nel 2017, le ricerche del Chartered Institute of Personnel and Development stimano, per il Regno Unito, circa 1,3 mln di gig workers, pari al 4% degli occupati[41].

---

[39] Si veda *https://www.eurofund.europa.eu/observatories/eurowork/industrial-relations-dictionary/gig-economy* e L. HYMAN, in *https://www.mckinsey.com/featured-insights/employment-and-growth/indipendent-work-choice-necessity-and-the-gig-economy*, 2018.

[40] Si vedano le ricerche condotte dal *team* di Cornell ILR University, *https://www.ilr.cornell.edu/news/gig-economy-data-hub.*

[41] M. FAIOLI (a cura di), *Il Lavoro nella Gig-Economy*, in *I Quaderni del Cnel*, 3, 2018.

Con ogni probabilità, la prolungata emergenza sanitaria, accelerando la trasformazione digitale e l'espansione dei modelli di attività basati su piattaforme digitali, ha contribuito a far emergere forme e condizioni di lavoro precarie, connotate dall'assenza di trasparenza, carenze di accordi contrattuali, con ricadute sulla tutela sociale, salute e sicurezza e, soprattutto, dalla impossibilità di inserimento nella tradizionale disciplina giuslavorista.

Con l'emersione dell'economia delle piattaforme, è stato necessario prevedere un ripensamento delle categorie tradizionali di lavoro, a partire dal binomio subordinazione-autonomia e dai relativi criteri discretivi.

Invero, talune attività "tradizionali", tra cui la consegna di cibo a domicilio o il trasporto passeggeri, vengono espletate dal prestatore mediante l'intermediazione di un'applicazione digitale per *smartphone* (lavoro *on demand*) e, in altri casi, una piattaforma virtuale (a titolo di esempio, Vicker, Cicogne o Task Rabbit) consente l'assegnazione di una serie di compiti, per lo più ripetitivi, (come l'inserimento di dati), da svolgersi mediante PC, ad una persona selezionata tra diversi potenziali individui candidatisi online.

Il *marketplace* delle piattaforme digitali beneficia, da una parte, delle richieste di lavoro (lavoratori/*riders*) e, dall'altra, delle richieste di servizi (ristorante che si associa alla piattaforma e consumatore che desidera acquistare cibo mediante *riders* ad una determinata ora).

Tra lavoratori, ristorante/pubblico esercizio e consumatore c'è la piattaforma digitale che gestisce le relazioni giuridiche e soddisfa i bisogni degli associati (ristoratore, esercente di attività commerciali) e del consumatore, evitando la congestione del mercato attraverso un algoritmo.

Tale algoritmo gestisce i lavoratori/*riders*, anticipa i bisogni dei consumatori, preallerta i ristoratori o soggetti simili associati alla piattaforma.

La *gig economy*, dunque, *"si sviluppa in un mercato anomalo, dove la prestazione marginale o occasionale di lavoro si svolge per il tramite di un ambiente digitale sofisticato che collega la domanda (crescente) all'offerta (crescente), che coordina le prestazioni di lavoro, che misura la qualità delle prestazioni di lavoro, che predice i bisogni dei consumatori e dei venditori di beni/servizi. Il prezzo ha un certo ruolo nella vicenda: non interessa al consumatore, se non nella misura in cui possa comparare un bene o un servizio (scelgo quel piatto di pasta da quel ristorante); non interessa al*

venditore di beni, il quale ha solo l'interesse a stare in una vetrina digitale; non interessa alla piattaforma digitale, la quale ha a disposizione molti lavoratori. Il corrispettivo, che viene a crearsi da questa vicenda giuridica, ha però ricadute sul costo del lavoro: più basso è il costo del lavoro, minori sono gli oneri della catena di valore (piattaforma, venditore, consumatore, riders)[42] *".*

2. Dalla subordinazione all'etero-organizzazione. Analisi giurisprudenziale.

In considerazione delle notevoli ricadute occupazionali, a livello nazionale, i giudici del lavoro italiani sono stati sinora investiti unicamente delle controversie concernenti la qualificazione del lavoro *on demand*, reso in particolare dagli ormai ben noti *riders*, mentre il *crowdwork* non è ancora emerso dalla sua dimensione virtuale[43].

La giurisprudenza ha, così, contribuito a delineare l'impatto di tali nuove modalità di relazioni contrattuali nella disciplina giuslavorista, considerando l'estrema flessibilità del modello analizzato.

Le controversie relative alla qualificazione del lavoro reso attraverso piattaforma hanno riguardato le prestazioni rese dai ciclofattorini (*riders*) incaricati tramite app del trasporto di cibo, in ambito prevalentemente urbano.

Pur considerando l'eterogeneità delle diverse piattaforme menzionate e dei *riders*, le prestazioni dei ciclofattorini presentano diversi elementi di analogia.

---

[42] M. FAIOLI (a cura di), *Il Lavoro nella Gig-Economy*, in *I Quaderni del Cnel*, 09.07.2019.

[43] Analizzando le line guida poste dall'Europa con l'Agenda sull'economia collaborativa – COM (2016) 356 e secondo il caso UBER con la sentenza della CGUE del 20.12.2017 (rinvio pregiudiziale operato dal Tribunale di Commercio n. 3 di Barcellona, con decisione del 16.07.2015) – C-434/15, la domanda partiva da un procedimento promosso da un'associazione professionale di conducenti di taxi, sostenitrice della violazione delle regole di "*leale concorrenza*" da parte della multinazionale californiana. I termini principali della questione vertevano sulla tipologia di servizio "*principalmente ed essenzialmente*" offerto: servizio di trasporto oppure mero servizio tecnologico di intermediazione fra utenti e conducenti, come affermato dai legali di UBER. La decisione della Corte, accogliendo il parere dell'Avvocato Generale, ha sancito che l'attività di intermediazione offerta tramite la app "UberPop" si configura, sebbene con modalità innovative, quale "*servizio nel settore dei trasporti*" e non come "*servizio di intermediazione elettronica o della società dell'informazione*". Ciò poiché il servizio di intermediazione è secondario rispetto al potere organizzativo che esercita su aspetti come i prezzi, gli orari di lavoro e le condizioni del veicolo e del servizio, nonché, in ultimo, sugli autisti stessi. Inoltre, la sentenza proseguiva nel senso della garanzia della compatibilità con il diritto UE di qualsiasi normativa nazionale che assoggetti l'attività di UBER, e non solo quella dei suoi autisti, a licenze o autorizzazioni. Come conseguenza, UBER è stata invitata a ridefinire i rapporti contrattuali con i propri conducenti, non qualificabili "prestatori liberi ed autonomi" come sostenuto dalla multinazionale. È stata, quindi, auspicata la pronta adozione di norme comuni a livello UE, derivandone l'adozione della Direttiva del Parlamento Europeo e del Consiglio del 20.06.2019 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:PE_43_2019_REV_1) che garantisce "*diritti minimi*" per i lavoratori che svolgono un'occupazione occasionale o a breve termine.

In merito alla qualificazione dei rapporti di lavoro dei rider, la giurisprudenza di merito esclude la natura subordinata del rapporto di lavoro, considerando che i *riders* stipulano con la piattaforma (id est con la società che gestisce la stessa) un contratto di lavoro autonomo, nella forma, a seconda delle circostanze, della "*collaborazione coordinata e continuativa*", del lavoro autonomo ex art. 2222 ss. C.c. o di un – atipico – rapporto di lavoro autonomo occasionale.

Gli accordi lasciano formalmente al lavoratore la scelta, oltre che di lavorare per altre piattaforme, di accettare o non accettare la proposte di consegna e, una volta accettato l'incarico, il *rider* si reca, mediante un mezzo proprio, con bauletto e pettorina recante l'effigie del committente, a ritirare il cibo che viene, poi, consegnato al domicilio del cliente della piattaforma, dietro pagamento del compenso a consegna o, alternativamente, a tempo, a seconda della piattaforma o del momento.

Per il tribunale di Torino, sez. lav., con la sentenza del 07.05.2018 n. 778, la libertà dei *riders* di accettare o non accettare gli incarichi sarebbe incompatibile con la subordinazione, risultando carente il potere della piattaforma di dirigere ed organizzare il lavoro.

Nel caso analizzato dalla corte territoriale, il rigetto delle domande dei fattorini di *Foodora*, tese a far riconoscere la natura subordinata del rapporto di lavoro, formalmente qualificato come contratto di collaborazione autonoma, più volte rinnovato, si fondava su due argomentazioni: la prima riguardava la volontarietà della prestazione, atteso che, secondo il giudicante, i *riders* sceglievano se mettersi a disposizione di *Foodora* per effettuare le consegne, indicando in quali turni erano disponibili ad effettuare il servizio.

La seconda era giustificata sull'assunto per il quale, durante l'istruttoria, era emersa la carenza di potere direttivo e/o gerarchico, discendendone la prova che i *riders* non erano sottoposti a nessun potere direttivo e/o disciplinare da parte di *Foodora*, godendo, anzi, di notevole autonomia nell'esecuzione della prestazione che doveva esclusivamente coordinarsi con le esigenze produttive del committente.

I lavoratori, dunque, non hanno l'obbligo di effettuare la prestazione lavorativa e la società, dal canto suo, non ha l'obbligo di riceverla; i *riders*, infatti, possono dare la loro disponibilità per uno dei turni indicati da *Foodora*, ma non sono obbligati a farlo; a sua volta, la società può o meno accettare la disponibilità data dai fattorini e inserirli nei turni da loro richiesti.

La non obbligatorietà della prestazione lavorativa, pertanto, vale ad escludere *in nuce* la subordinazione perché l'etero direzione è incompatibile con la libertà della parte che deve rendere la prestazione di rifiutarla.

Secondo la categorica affermazione della Suprema Corte, nell'individuazione degli elementi che connotano il rapporto di lavoro subordinato rispetto al lavoro autonomo, "*l'elemento che contraddistingue il rapporto di lavoro subordinato rispetto al rapporto di lavoro autonomo è il vincolo di soggezione personale del lavoratore al potere organizzativo, direttivo e disciplinare del datore di lavoro, con conseguente limitazione della sua autonomia ed inserimento nell'organizzazione aziendale, mentre altri elementi, quali l'assenza di rischio, la continuità della prestazione, l'osservanza di un orario e la forma della retribuzione, pur avendo natura meramente sussidiaria e non decisiva, possono costituire indici rivelatori della subordinazione, idonei anche a prevalere sull'eventuale volontà contraria manifestata dalle parti, ove incompatibili con l'assetto previsto dalle stesse"*[44].

Del pari, il giudicante decideva per l'inapplicabilità dell'art. 2 del d.lgs. n. 81/2015, che introduce una definizione più ristretta di subordinazione rispetto all'art. 2094 c.c., in quanto "i *rapporti di collaborazione che si concretano in prestazioni di lavoro esclusivamente personale, continuative e le cui modalità di esecuzione sono organizzate dal committente anche con riferimento ai tempi e al luogo di lavoro*"[45].

La prestazione, pertanto, deve essere disciplinata dal committente anche nei tempi e nei luoghi della prestazione, circostanza che, invece, non ricorre nel rapporto di lavoro con i ciclofattorini i quali gestiscono in autonomia i tempi di lavoro e di riposo (cfr. Trib. di Milano sez. lav. 10.09.2018 n. 1853).

Contrariamente a quanto aveva sostenuto il Tribunale di Torino, la Corte d'Appello, con sentenza del 04.02.2019 n. 26, ha considerato applicabile alla fattispecie la previsione contenuta nell'art. 2, co. I, d.lgs. 81/2015, considerandola una norma precettiva,

[44] Cass. Civ., sez. lav., 14.06.2018 n. 15631; Cass., sez. Lav., 11.07.2018 n. 18253; Cass., sez. lav., 11.07.2018 n. 18254.

[45] La disciplina di cui all'art. 2 co. I d.lgs. 81/2015 richiede, per la sua configurazione, a) personalità della prestazione, che si realizza quando l'attività è svolta esclusivamente attraverso le energie del lavoratore che non può essere sostituito né può avvalersi di collaboratori; b) continuità della prestazione, intesa come apprezzabile svolgimento nel tempo dell'impegno lavorativo del collaboratore in favore del committente, ricorrendo, quindi, allorquando la prestazione non sia episodica ma perduri nel tempo e importi un impegno del prestatore, in favore del committente, costante anche se no in lassi temporali consecutivi; c) organizzazione dei tempi e delle modalità di lavoro da parte del committente, consistente nel potere unilaterale del committente di conformare la prestazione lavorativa anche nel corso del suo svolgimento.

della quale spetta al giudice fornire l'interpretazione "*stante il sottile confine tra il dettato della stessa e il disposto dell'art. 2094 c.c.".*

La Corte di secondo grado, invero, riteneva che la richiamata disposizione individui un *tertium genus,* tra il rapporto di lavoro subordinato e le collaborazioni ex art. 409, n. 3 c.p.c., poiché la collaborazione è etero-organizzata, "*quando è ravvisabile un'effettiva integrazione funzionale del lavoratore nell'organizzazione produttiva del committente*", il quale ha il potere di "determinare le modalità di esecuzione della prestazione lavorativa del collaboratore e cioè la possibilità di stabilire i tempi e i luoghi di lavoro".

L'etero-organizzazione, di cui alla previsione dell'art. 2 co. I d.lgs. 81/2015, va distinta sia dal potere direttivo, che caratterizza il lavoro subordinato, sia dal coordinamento di cui all'art. 409 n. 3 c.p.c., le cui modalità, come precisa la Corte, sono stabilite consensualmente, mentre quelle di esecuzione della prestazione sono definite autonomamente dal collaboratore.

Per la Corte, dunque, il lavoratore etero-organizzato resta, comunque, un prestatore d'opera, al quale si applica, ai sensi del suddetto art. 2, co. I, la disciplina del lavoro subordinato, in particolare per quello che riguarda "*sicurezza e igiene, retribuzione diretta e differita (quindi inquadramento professionale), limiti di orario, ferie e previdenza*".

Ciò che il giudice di appello ha posto in evidenza consiste nella circostanza per la quale non conta "*il fatto che il lavoratore sia libero o meno di accettare l'offerta e di presentarsi o non presentarsi al lavoro e senza necessità di giustificazione*", quanto le modalità con cui concretamente si svolge la prestazione di lavoro dopo che sia intervenuta l'accettazione.

A tal punto, la Suprema Corte interveniva, con sentenza del 24.01.2020 n. 1663, modificando parzialmente la motivazione cui era pervenuta la Corte d'Appello di Torino, negando che la succitata disposizione legislativa dell'art. 2, co. I, d.lgs. 81/2015, istituisse un tipo legale intermedio tra il lavoro subordinato e il lavoro autonomo, cioè del lavoro etero-organizzato, sostenendo, per contra, che la stessa estendesse il campo di applicazione di tutte le protezioni del lavoro subordinato – compresa la disciplina dei licenziamenti – ad un'area assai ampia del lavoro autonomo, quella caratterizzata dalla etero-organizzazione della prestazione.

La Corte di legittimità, dunque, riassumeva il dibattito – non ancora esaurito – che ha accompagnato l'entrata in vigore del d.lgs. n. 81/2015, art. 2, co. I, evidenziando a)

una prima via, che segue il metodo qualificatorio, di riconoscere alle prestazioni rese dai lavoratori delle piattaforme digitali i tratti della subordinazione, sia pure ammodernata ed evoluta; b) una seconda via che immagina l'esistenza di una nuova figura intermedia tra subordinazione ed autonomia, caratterizzata dall'etero-organizzazione e che trova nell'art. 2, co. I, d.lgs. 81/2015, il paradigma legale (teoria del *tertium genus* o del lavoro etero-organizzato); c) una terza possibilità di ricondurre lo schema nell'ottica del lavoro autonomo dove, tuttavia, i modelli interpretativi si diversificano notevolmente essendo, peraltro, tutti riconducibili nell'ambito di una nozione ampia di parasubordinazione; d) infine, un approccio "*rimediale*" che rinviene la possibilità di applicare una tutela "rafforzata" nei confronti di alcune tipologie di lavoratori (quali quelli delle piattaforme digitali considerati "deboli") cui estendere le tutele dei lavoratori subordinati.

Orbene, la Corte di legittimità ha ritenuto che "*non ha senso interrogarsi se queste forme di collaborazione così connotate [...] siano riconducibili nel campo della subordinazione o dell'autonomia perché ciò che conta è che per esse, in una terra di mezzo dai confini labili, l'ordinamento ha stabilito espressamente l'applicazione delle norme sul lavoro subordinato*" e che *"quando l'etero-organizzazione accompagnata dalla personalità e dalla continuità della prestazione rende il collaboratore comparabile ad un lavoro dipendente, si impone una protezione equivalente e quindi il rimedio dell'applicazione integrale della disciplina del lavoro subordinato*".

Con specifico riferimento alla vicenda dei *riders*, costoro sottoscrivono contratti di collaborazione relativamente ai quali si comportano quali meri contraenti d'opera o di servizio perché formalmente sono liberi di accettare il singolo incarico, ma nella sostanza, una volta accettato ciascun incarico, la loro attività è regolata da un "*algoritmo che esercita un controllo pervasivo sull'attività svolta dal singolo rider e penalizza quei prestatori che non si adeguano al modello ideale di produttore (che presuppone la sottoposizione a turni massacranti di lavoro), stila la classifica dei più meritevoli e traccia le prestazioni dei singoli e le confronta. E quindi la piattaforma tramite l'algoritmo controlla la prestazione e sanziona i comportamenti non conformi a determinati standard*"[46].

[46] O. MAZZOTTA, *L'inafferrabile etero-direzione: a proposito dei ciclofattorini e modelli contrattuali*, in *Labor*, 1, 2020.

Trattasi, pertanto, di un lavoro fortemente vincolato, nonostante fino all'accettazione dell'incarico il *rider* possa essere libero ed autonomo oppure il lavoro de quo può articolarsi in una serie di incarichi collegati da un nesso di continuità perché risponde sempre alla chiamata e, in questo caso, può qualificarsi come contratto di durata perché soddisfa un interesse durevole del committente.

Al contempo, il rapporto del *rider* può essere, certamente, discontinuo se il lavoratore non risponde sempre alla chiamata, trovando, dunque, applicazione le tutele minime dettate dagli artt. 47-*bis* e ss. del citato d.lgs. che non menzionano e non presuppongono la continuità del rapporto di lavoro del *rider*.

Se si accoglie come criterio scriminante la continuità del rapporto, a tale ultima tipologia di rider che non presta attività in forma continuativa perché sceglie di volta in volta se rispondere alla chiamata e quindi di rendere la prestazione si applicano esclusivamente le tutele di cui agli art. 47-*bis* e ss[47]. Per contra, se il rapporto di lavoro del ciclofattorino è continuativo, allo stesso potrà essere applicato l'art. 2, 1 co.

Ne deriva che il Legislatore abbia voluto rafforzare la libera scelta del rider di accettare o meno la chiamata, stabilendo che "*l'esclusione dalla piattaforma e le riduzioni delle occasioni di lavoro ascrivibili alla mancata accettazione della prestazione sono vietate"* (art. 47-quinquies, 2 co.)[48].

La Corte osservava, infine, che l'art. 47-bis, comma 2, d.lgs. n. 81/2015, chiarisce che, ai fini dell'applicazione dei livelli minimi di tutela per i lavoratori autonomi addetti alle consegne di beni tramite piattaforme anche digitali, si considerano piattaforme digitali «i *programmi e le procedure informatiche utilizzati dal committente che, indipendentemente dal luogo di stabilimento, sono strumentali alle attività di consegna di beni, fissandone il compenso e determinando le modalità di esecuzione della prestazione*».

---

[47] A. PERULLI, *Il Diritto del Lavoro "oltre la subordinazione": le collaborazioni etero-organizzate e le tutele minime per i riders autonomi,* in *Working Paper CSDLE* "*Massimo D'Antona".IT,* 2020, P. 410, il quale, da una parte, afferma che «*la continuità o meno della prestazione non può certo essere un criterio ragionevole per differenziare in modo così radicale i trattamenti» (p. 21, nota 27), dall'altra, in modo non dissimile da quanto sopra riferito, chiarisce che «mentre il rapporto di lavoro etero-organizzato è continuativo, l'art. 47 bis non richiama questo elemento, onde, benché tenue, un primo criterio distintivo tra le due fattispecie e relative discipline potrebbe essere rintracciato in questa distinzione tra prestazioni continuative e lavoro autonomo occasionale*».

[48] Nel dettare la definizione di piattaforma utile ai fini dell'applicazione delle tutele, il co. II dell'art. 47-bis del d.lgs. 81/2015 specifica che si tratta di "programmi" e delle "procedure informatiche" che, "*indipendentemente dal luogo di stabilimento, sono strumentali all'attività di consegna dei beni, fissandone il compenso e determinando le modalità di esecuzione della prestazione"*.

La previsione del potere della piattaforma di determinare le modalità esecutive della prestazione rivela certamente un difetto di coordinamento tra norme, in quanto si sovrappone, sia in astratto sia in concreto, con l'ambito di applicazione dell'art. 2, comma 1, e persino con l'etero-direzione ex art. 2094 c.c.

Ma poiché non sembra realistico arrivare ad un'*interpretatio abrogans*, e comunque non si può considerare residuale l'ambito di applicazione delle norme degli artt. 47-bis e ss., risulta ragionevole utilizzare il criterio della continuità-occasionalità della prestazione per distinguere i *riders* che prestano la loro opera continuativamente, ai quali si applica l'art. 2, 1 co. (seconda parte aggiunta dal d.lgs. n. 101/2019), da quelli che la prestano occasionalmente, ai quali si applicano gli artt. 47, comma 2-bis, e ss[49].

3. Il "ritorno" alla natura subordinata del rapporto di lavoro dei riders addetti al "food delivery".

Se la Corte, dunque, con la suddetta pronuncia, ha reputato di optare, ai fini dell'inquadramento dei ciclofattorini, nella figura delle collaborazioni etero-organizzate, la successiva sentenza di merito del Tribunale di Palermo del 24.11.2020 n. 3570 ha, invece, considerato più adeguata la fattispecie descritta ex art. 2094 c.c., corrispondente al rapporto di lavoro subordinato a tempo pieno e indeterminato.

Il ricorrente, rider per Foodihno s.r.l., sosteneva che la società non consentisse alcuna autonomia in sede di ritiro e consegna dei prodotti e nella determinazione del corrispettivo, dando luogo ad una subordinazione in fase di attuazione del rapporto, e che tutta l'attività del ciclofattorino è caratterizzata dall'assenza di autonomia, da un puntuale e dettagliato coordinamento da parte della resistente e da sanzioni e penalizzazioni atipiche in caso di scostamento dal modello organizzativo.

L'attività del rider andava qualificata alla stregua del lavoro subordinato atteso che la sua prestazione era costantemente gestita e diretta dalla piattaforma digitale dalla fase iniziale di accettazione dell'ordine al suo ritiro (cd. Presa in consegna) sino al recapito e alla rimessa del denaro.

A tal fine, il giudice palermitano riprendeva la già ricordata pronuncia della Corte di Giustizia UE del 20.12.2017, C-434/15, nel caso che aveva coinvolto la società Uber System Spain citata in giudizio da Elite Taxi, significativa per la qualificazione come

[49] G. SANTORO-PASSARELLI, *L'interpretazione dell'art. 2 co. I del d.lgs. 81/2015 e i Riders nella sentenza della Cassazione n. 1663/2020*, in *Diritto delle Relazioni Industriali*, 2, 2020.

attività di impresa delle piattaforme "*aventi ad oggetto la messa in contatto mediante un'applicazione per smartphone, dietro retribuzione, di conducenti non professionisti, che utilizzano il proprio veicolo, con persone che desiderano effettuare uno spostamento nell'area urbana*" nonché le precedenti sentenze del Tribunale di Milano del 15.06.2015 n. 23, del Tribunale di Torino del 01.03.2017 n. 1553 e della Corte d'Appello di Parigi (Cour d'Appel de Paris del 10.01.2019 n. 18/08357) che chiariva che *"(...le chauffeur...) a ainsi intègrè un service de prestation de transport crèè et entièrement organisè par la sociètè Uber BV, qui n'existe que grace à cette plateforme, service de transport à travers l'utilisation duquel il ne constitue aucune clientèle propre, ne fixe pas librement ses tarifs ni les conditions d'exercice de sa prestation de transport, qui sont entièrement règis par la sociètè Uber BV*" e della Cour de Cassation, Chambre Sociale, 04.03.2020 n. 374, che evidenziava che il prestatore di lavoro non può considerarsi quale partner commerciale; al contrario, nel momento della stipulazione del contratto, egli aderisce ad un servizio di trasporto interamente organizzato da Uber attraverso la piattaforma digitale e i sistemi di elaborazione algoritmici che ne determinano il funzionamento.

L'autista che ricorre all'infrastruttura tecnologica non ha la possibilità di crearsi una propria clientela nè di determinare liberamente le tariffe da applicare e, in tal modo, colloca la propria attività lavorativa entro un quadro di regole determinato dall'esterno.

Ed ancora, valeva il richiamo anche alle altre pronunce estere che hanno ugualmente qualificato il lavoro dei riders nei termini della subordinazione[50] o nei termini dell'autonomia[51].

Rispetto alle sentenze sopra rammentate (cfr. Corte d'Appello di Torino del 04.02.2019 n. 26. confermata dalla Corte di Cassazione con la sentenza n. 1663/2020), tuttavia, si operava una valutazione di un solo segmento del rapporto di lavoro con la piattaforma, quello iniziale, omettendo di addentrarsi nella valutazione anche dell'altro segmento, rappresentato dalla fase esecutiva della prestazione.

Osservava il giudicante che "*la prestazione dei rider e del ricorrente in particolare risulta completamente organizzata dall'esterno (etero-organizzata), e, d'altra parte,*

[50] Cfr. 33 a VARA DO TRABALHO DE BELO HORIZONTE, 14.02.2017, n. 0011359-34.2016.5.030112 RIDL, 2017, II; JUZGADO DE LO SOCIAL DE VALENCIA, 01.06.2018 N. 244; SALA DE LO SOCIAL PLENO Sentencia nùm. 805/2020 Fecha de sentencia 25.09.2020.

[51] Cfr. SUN YONGLING, V. BEIJING YIXING, *Automotive Technology Development Services Ltd Labpur Dispute Beijing First Intermediate People's Court*, Civil Judgement, 2015, YI ZHONG MIN ZHONG ZI DI NO, 176; JUSGADO DE LO SOCIAL N. 39 REFUERZO MADRID N. 284/2018; TRIBUNAL SUPERIOR DE JUSTICIA DE MADRID N. 715/2019.

che la libertà del rider, segnatamente del ricorrente, di scegliere se e quando lavorare, su cui si fonda la natura autonoma della prestazione (anche sulla scorta della citata decisione della Corte di Giustizia), non è reale, ma solo apparente e fittizia, poiché, a tutto concedere, il lavoratore può scegliere di prenotarsi per i turni che la piattaforma (e quindi il datore di lavoro che ne è titolare o ne ha il controllo) mette a sua disposizione in ragione del suo punteggio. Egli, inoltre, per poter realmente svolgere la prestazione, deve essere loggato nel periodo di tempo che precede l'assegnazione della consegna, avere il cellulare carico in misura almeno pari al 20% e trovarsi nelle vicinanze del locale presso cui la merce dev'essere ritirata, poiché altrimenti l'algoritmo non lo selezionerà, benché egli avesse prenotato e non disdetto lo slot, con la conseguenza che, in verità, non è lui che sceglie quando lavorare o meno, poiché le consegne vengono assegnate dalla piattaforma tramite l'algoritmo, sulla scorta di criteri del tutto estranei alle preferenze e allo stesso generale interesse dal lavoratore (…)".
In sostanza, è noto che le piattaforme, inclusa la società coinvolta nel processo di Palermo, stabiliscono fasce orarie – slot nel gergo maggiormente ricorrente nelle piattaforme di consegna di pasti e bevande – all'interno delle quali si inseriscono i *riders* e i drivers in base a meccanismi di auto assegnazione, influenzati tuttavia anche da scelte dell'impresa, mediante l'applicazione di algoritmi[52].
Ed infatti, "*al di là dell'apparente e dichiarata (in contratto) libertà del rider, e del ricorrente in particolare, di scegliere i tempi di lavoro e se rendere o meno la prestazione, l'organizzazione del lavoro operata in modo esclusivo dalla parte convenuta sulla piattaforma digitale nella propria disponibilità si traduce, oltre che nell'integrazione del presupposto della etero-organizzazione, anche nella messa a disposizione del datore di lavoro da parte del lavoratore delle proprie energie lavorative per consistenti periodi temporali (peraltro non retribuiti) e nell'esercizio da parte della convenuta di poteri di direzione e controllo, oltre che di natura latamente disciplinare, che costituiscono elementi costitutivi della fattispecie del lavoro subordinato ex art. 2094 c.c.".*
Ciò detto, in disparte le ricognizioni operate in giurisprudenza circa la qualificazione più adatta da attribuire ai rapporti *de quibus*, se in termini di sussunzione della fattispecie nell'autonomia o nella subordinazione, sarebbe opportuno porre in primo piano

[52] G. CAVALLINI, *Foodora, Deliveroo & Co. Le fattispecie della gig-economy italiana tra previsioni contrattuali e concrete modalità di esecuzione del rapporto*, in *Impresa, lavoro e non lavoro nell'economia digitale*, a cura di C. ALESSI, M. BARBERA, L. GUAGLIANONE, *Atti del convegno di Brescia* 12-13 ottobre 2017, Bari, 2019, 712 ss.

gli strumenti per la tutela dei diritti. In questo modo si potrebbe superare la pretesa totalizzante e unitaria tipica della fattispecie giuridica.

Riferimento in tal senso dovrebbero essere i criteri ordinatori contenuti nei principi costituzionali relativi alla materia del lavoro, sanciti anche dalle fonti internazionali e nello specifico l'art. 36 Cost., per garantire un compenso salariale minimo, il principio della tutela della salute per sancire gli standard fondamentali di sicurezza sul lavoro, il principio di pari dignità e non discriminazione per proteggere i lavoratori da pratiche discriminatorie e lesive della dignità e della privacy, e i principi di libertà e di organizzazione sindacale[53].

Nel medesimo senso, l'accademico Ichino[54] riteneva l'opportunità di prescindere dalla qualificazione come subordinati o autonomi per i *platform workers*, almeno nella parte indispensabile delle protezioni compatibili con la peculiare forma di organizzazione del loro lavoro, evitando di imporre gli schemi tradizionalmente propri del lavoro subordinato.

A prescindere, pertanto, dalla qualificazione giuridica del rapporto di lavoro, si ritiene che occorra garantire il rispetto dei principi di correttezza e buona fede, suggerendosi alcune proposte tese a garantire trasparenza e trasferibilità del rating, trasparenza nella gestione dell'account (specialmente con riferimento alla possibilità di disattivazione), limiti alle modifiche unilaterali del contratto, il riconoscimento di un livello minimo di protezione (mediante il richiamo ai principi ed ai diritti fondamentali dell'Organizzazione Internazionale del Lavoro – OIL).

Tale livello minimo dovrebbe prevedere altresì l'accesso a diritti fondamentali quali la libertà di associazione e il diritto alla contrattazione collettiva, la libertà dal lavoro forzato e minorile e il diritto a non essere discriminati[55].

---

[53] T. TREU, *Il Lavoro nella Gig-Economy*, M. FAIOLI (a cura di), in *I Quaderni del C.N.E.L.*, 2017, 09.07.2019.

[54] P. ICHINO, *Il Lavoro nella Gig-Economy*, M. FAIOLI (a cura di), in *I Quaderni del C.N.E.L*, 2018, 09.07.2019.

[55] Cfr. V. DE STEFANO, *Il Lavoro nella Gig-Economy*, M. FAIOLI (a cura di), in *I Quaderni del C.N.E.L*, 2017, 09.07.2019.

GLI ALGORITMI ALLA BASE DI DECISIONI PUBBLICHE FRA INTELLIGENZA ARTIFICIALE, TUTELA DEI DIRITTI E REGOLE DI BUONA AMMINISTRAZIONE. MEDIANTE LA DISCREZIONALITÀ UMANA LE FEATURES TECNOLOGICHE VANNO TEMPERATE DAI PRINCIPI DI RAGIONEVOLEZZA, TRASPARENZA E MOTIVAZIONE

di Sergio Guida

SOMMARIO. 1. Intelligenze artificiali e algoritmi. 2. La tutela dell'interesse pubblico tramite il ricorso ad algoritmi: esperienze internazionali. 3. Esperienze nel nostro Paese e garanzie giurisprudenziali. 4. Conclusioni.

The need for an effective control of the decision-making algorithms used in the PA raises fundamental legal questions that are resolved differently depending on the national system. Among these, the possibility of reviewing the reasonableness of the administrative decision, the possible violation of the principle of transparency and the lack of motivation. But before that there is the relationship between law and technology, with the difficulty of codifying something that is subject to a very rapid capacity for change. On the other hand, addressing the structural, social, political and economic impacts of AI use will ensure that the law is 'future-proofed' and prioritises the protection of fundamental rights.

1. Intelligenze artificiali e algoritmi.

I sistemi decisionali automatizzati (*Automated decision-making, ADM*)[56] si basano su *software* che supportano o sostituiscono elementi del processo decisionale umano nell'attuazione del diritto. I sistemi ADM sono implementati in un numero crescente

[56] Un "sistema decisionale automatizzato" può essere definito come un software, un sistema o un processo che mira ad aiutare o sostituire il processo decisionale umano. Si veda ad es. RASHIDA RICHARDSON, *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI Now Institute, December 4, 2019 in https://ainowinstitute.org/ads-shadowreport-2019.pdf, pag.7.

di aree e la migliore disponibilità di informazioni e la potenza di calcolo avanzata per elaborare tali informazioni produce vantaggi per il processo decisionale[57].

Le tecnologie ADM influenzano le procedure decisionali e di regolamentazione principalmente per le loro caratteristiche tecnologiche, la relazione tra ADM e base di dati, nonché la relazione tra ADM e gli elementi umani del processo decisionale. Esse si basano su software per automatizzare, accelerare e scalare l'analisi dei dati. I dati estratti da uno o più *database* su larga scala vengono utilizzati per calcolare le probabilità in base a passaggi predefiniti per soddisfare determinati passi di un programma[58].

Il software può anche contenere uno o più elementi di intelligenza artificiale (IA).

L'IA è descritta dalla bozza di "Regolamento su un approccio europeo per l'intelligenza artificiale" come *"una famiglia di tecnologie in rapida evoluzione che può contribuire a un'ampia gamma di vantaggi economici e sociali"*[59]. L'utilizzo di IA permette di inferire relazioni complesse e non lineari dai dati che il software analizza, per raggiungere un obiettivo specifico identificando e, se necessario, perfezionando automaticamente le operazioni di un sistema.

Vari approcci alla programmazione dell'IA si stanno evolvendo e in tale contesto è emerso che gli effetti da essi scaturenti non sono uguali.

- Ad esempio, un approccio alla programmazione dell'IA si concentra sui *"sistemi simbolici"*: in tal caso si richiede che il software fornisca specifiche predefinite, passo dopo passo, delle regole, dei fatti e delle strutture che definiscono le caratteristiche dei calcoli effettuati dal programma. L'IA simbolica è legata alle rappresentazioni fornite dagli esseri umani che intraprendono la programmazione e, pertanto, consente, in linea di principio, di fornire spiegazioni sull'esito di calcoli specifici e di documentare requisiti propri del programma.
- Altri approcci all'IA si basano sull'apprendimento automatico (*machine learning*), che addestra un sistema informatico su una serie di input e sui risultati previsti. Ad esempio, l'input potrebbe consistere nelle caratteristiche di colui che richiede un visto di viaggio, mentre il risultato consisterebbe nella decisione di concedere o

[57] Cfr. HERWIG C.H. HOFMANN, *An Introduction to Automated Decision Making (ADM) and Cyber-Delegation in the Scope of EU Public Law*, Law Working Paper Series, Paper number 2021-008, Université du Luxembourg, 23 June 2021, Electronic copy available at: https://ssrn.com/abstract=3876059, pag.1.

[58] *Ibidem*, pag.2.

[59] Cfr. Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione - COM/2021/206 final, Bruxelles, 21.4.2021 in https://eur-lex.europa.eu/legal-content/IT/TXT/?uri= CELEX%3A52021PC0206, pag.2.

rifiutare il visto. Il software di apprendimento automatico utilizza le informazioni fornite nei dati di addestramento e il processo decisionale passato per calcolare parametri in grado di collegare gli input agli output. Questa forma di IA (apprendimento supervisionato) non ha bisogno di essere basata su esplicite "regole *if-then*", ma calcola sulla base di input non visti in precedenza il possibile risultato. Dal punto di vista della responsabilità del processo decisionale, questo tipo di approccio richiede una funzione più chiaramente definita di *reporting* degli approcci al processo decisionale rispetto all'IA simbolica, che è più spiegata da disposizioni *if-then* di algoritmi. Nell'apprendimento automatico persistono problemi di comprensibilità poiché i modelli di apprendimento automatico si basano su vari calcoli che rappresentano in primo luogo gli input e il modo in cui vengono pesati, in secondo luogo gli output che il sistema produce e, in terzo luogo, il modello di apprendimento automatico effettivo, tanto che questa programmazione potrebbe soffrire di debolezze nell'identificare le relazioni tra cause ed effetti.

- Un terzo approccio consiste nello sviluppo di sistemi di intelligenza artificiale per produrre risultati basati sul cosiddetto *"apprendimento non supervisionato"*. In tal modo, il software è programmato per produrre un possibile output, ma il programma non richiede esempi etichettati relativi all'input. Questa tecnologia AI è stata creata per sviluppare il riconoscimento dei modelli, ad esempio per rilevare anomalie, per migliorare la sicurezza informatica o per la segmentazione dei clienti nel marketing dei prodotti. Tale intelligenza artificiale può essere molto utile nella *"definizione dell'agenda"* e nell'avvio di procedure amministrative, si pensi, ad esempio alla vigilanza dei mercati finanziari, dove è necessario analizzare grandi quantità di dati senza chiare indicazioni precedenti relative all'input. Il controllo degli esiti di tale intelligenza artificiale tende a essere più difficile rispetto agli approcci di apprendimento automatico poiché ci sono meno collegamenti chiari tra input e output[60].

Dal punto di vista operativo, i sistemi decisionali automatizzati (ADM) si riferiscono a tecnologie basate sui dati e utilizzate per automatizzare procedure, pratiche o politiche *human-centered* allo scopo di prevedere, identificare, sorvegliare, rilevare e prendere di mira individui o comunità. In particolare, queste tecnologie sono utilizzate dalle

[60] Cfr. HERWIG C.H. HOFMANN, *An Introduction to Automated Decision Making (ADM) and Cyber-Delegation in the Scope of EU Public Law*, Law Working Paper Series, Paper number 2021-008, Université du Luxembourg, 23 June 2021, Electronic copy available at: https://ssrn.com/abstract=3876059, pagg.3-4.

agenzie governative per allocare risorse governative limitate (ad esempio, benefici pubblici o servizi sanitari); prevedere e presumibilmente prevenire rischi specifici o esiti negativi; rimuovere o ridurre la discrezionalità dall'attuale processo decisionale umano; fornire analisi che non possono essere eseguite dagli esseri umani. Queste tecnologie sono quindi applicate in campi come 'polizia predittiva', valutazione del rischio preprocessuale, algoritmi di corrispondenza dei compiti scolastici, sistemi di rilevamento delle frodi, sistemi di gestione del traffico, strumenti di screening o riconoscimento facciale.

Se però le sfide etiche non vengono affrontate in modo sufficiente, una mancanza di fiducia del pubblico nell'ADS potrebbe ostacolare l'adozione di tali sistemi che, a sua volta, porterebbe a significativi costi di opportunità sociali dovuti al sottoutilizzo delle tecnologie disponibili e ben progettate: affrontare le sfide etiche poste dall'ADS sta quindi diventando un prerequisito per una buona *governance* nelle società dell'informazione[61]. Sfortunatamente, i tradizionali meccanismi di *governance* progettati per supervisionare i processi decisionali umani spesso falliscono quando applicati all'ADM.

Un esempio: l'articolo 22, paragrafo 1, del Regolamento generale sulla protezione dei dati dell'Unione europea (GDPR) conferisce alle persone il diritto di non essere soggette a determinati tipi di decisioni completamente automatizzate. Al paragrafo 3 prevede poi una serie di garanzie che i titolari del trattamento devono attuare nel caso in cui gli interessati acconsentano a tale decisione (articolo 22, paragrafo 2, lettera c)). Una di queste, come precisato in un considerando non vincolante (considerando 71), conferisce all'interessato il diritto di ottenere una spiegazione della decisione raggiunta. Il termine "*explanation"* è sufficientemente ambiguo da comprendere tipi di spiegazione che mirano alla parte più profonda di uno strumento di decisione.

È allora istruttivo confrontare i tipi di spiegazione previsti per i sistemi predittivi con quelli forniti abitualmente dagli agenti umani. È vero che questi ultimi sono in grado di motivare le proprie decisioni, ma questo non corrisponde esattamente a come illuminare i processi cognitivi che portano a una conclusione.

[61] Cfr. JAKOB MÖKANDER, JESSICA MORLEY, MARIAROSARIA TADDEO,LUCIANO Floridi, *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations*, Science and Engineering Ethics (2021) 27:44 https://doi.org/10.1007/s11948-021-00319-4, 6 July 2021 in https://link.springer.com/content/pdf/10.1007/s11948-021-00319-4.pdf, pag.43.

I processi cognitivi alla base delle scelte umane, soprattutto in quanto elementi cruciali di intuizione, impressione personale e intuizioni inarticolate, che guidano gran parte della deliberazione, sono tutt'altro che trasparenti[62]. Le arene decisionali che richiedono, ad esempio, la valutazione della probabilità di recidiva, o la capacità di rimborsare un prestito, il più delle volte comportano il ricorso a fattori 'subdoxastici', ovvero fattori al di sotto del livello di convinzione cosciente[63].

In effetti, la delega dei compiti all'ADS riduce la sfera della deliberazione etica nei processi decisionali; in pratica, le norme che un tempo erano aperte all'interpretazione da parte dei decisori umani sono ora incorporate nell'ADS. Da una prospettiva etica, questo sposta il focus della deliberazione etica dalle specifiche situazioni decisionali ai modi in cui gli ADMS sono progettati e implementati[64].

2. La tutela dell'interesse pubblico tramite il ricorso ad algoritmi: alcune esperienze internazionali.

I governi democratici in tutto il mondo si affidano sempre più all'intelligenza artificiale. I dipartimenti di polizia negli Stati Uniti, nel Regno Unito e altrove hanno iniziato ad utilizzare la tecnologia di riconoscimento facciale per identificare potenziali sospetti. Giudici e tribunali hanno iniziato a fare affidamento sull'apprendimento automatico per guidare le decisioni sulle sentenze. Nel Regno Unito, un'autorità locale

[62] Si veda anche ad es. EYAL AHARONI, CHADD FUNK ET AL., *Can Neurological Evidence Help Courts Assess Criminal Responsibility? Lessons from Law and Neuroscience*, Ann. New York Academy of Sciences.1124:145–160 (2008).
Doi: 10.1196/annals.1440.007, https://pubmed.ncbi.nlm.nih.gov/18400929/, dove, a pag.154 si legge "La capacità di diventare consapevoli delle proprie intenzioni prima che abbiano portato all'azione sembra necessaria per un senso di 'agentività' (*agency*), l'esperienza di essere la fonte causale delle proprie azioni. Per 'conoscere la natura e la qualità del suo atto', un individuo dovrebbe presumibilmente riconoscere che queste azioni sono state causate da se stesso piuttosto che da qualcun altro".

[63] Cfr. "Le idee inconsce costituiscono ciò che Peirce chiamava un fondamento psicologico per le abitudini: 'l'idea generale di Peirce.. è già determinante degli atti futuri in una misura in cui non è ora cosciente'. Ha usato i termini ampliativo ed esplicativo per differenziare tra i modi di ragionamento che mirano non solo ad aumentare chiaramente le conoscenze di base ma, al contrario, a esplicitare la conoscenza nascosta o implicita, rendere manifesto ciò che è latente e inconscio, cioè il suo contenuto subdossastico e preconcettuale, cioè presimbolico", come si legge in INNA SEMETSKY, *Peirce's Semiotics, Subdoxastic Aboutness, and the Paradox of Inquiry*, Educational Philosophy and Theory, Vol. 37, No. 2, © 2005 Philosophy of Education Society of Australasia, electronic copy in https://ahmadriza.files. wordpress.com/2007/11/social-semiotics2.pdf, pagg.234-235.

[64] Cfr. JAKOB MOKANDER, JESSICA MORLEY, MARIA ROSARIA TADDEO, LUCIANO FLORIDI, *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations,* Science and Engineering Ethics (2021) 27:44 https://doi.org/10.1007/s11948-021-00319-4, 6 July 2021 in https://link.springer.com/content/pdf/10.1007/s11948-021-00319-4.pdf, cit., pag. 44.

britannica su tre utilizza algoritmi o strumenti di apprendimento automatico per prendere decisioni su questioni come le richieste di prestazioni sociali. Questi usi governativi dell'IA sono abbastanza diffusi tanto che in molti si chiedono se sia arrivata l'era del governo per algoritmo[65].

Molti critici hanno infatti espresso preoccupazione per l'uso in rapida espansione del processo decisionale automatizzato in aree sensibili della politica come la giustizia penale e il benessere. La preoccupazione più spesso espressa è inerente alla questione del pregiudizio: quando i sistemi di apprendimento automatico vengono addestrati su set di dati distorti, incorporeranno inevitabilmente nei loro modelli le disuguaglianze sociali alla base dei dati[66]. Le comunità della scienza dei dati e dell'intelligenza artificiale sono ora molto sensibili ai problemi di distorsione dei dati e, di conseguenza, hanno iniziato a concentrarsi molto più intensamente sull'etica dell'intelligenza artificiale[67]. Allo stesso modo, singoli governi e organizzazioni internazionali hanno pubblicato dichiarazioni di principio intese a disciplinare l'uso dell'IA[68].

Un principio comune dell'etica dell'IA è la spiegabilità: il rischio di produrre un'IA che rafforzi i pregiudizi sociali ha spinto a richiedere una maggiore trasparenza sui processi decisionali algoritmici o di apprendimento automatico e sui modi per comprendere e controllare come un agente di intelligenza artificiale arriva alle sue decisioni o classificazioni. Poiché l'uso dei sistemi di intelligenza artificiale prolifera, essere in grado di spiegare come funziona un determinato modello o sistema è fondamentale, soprattutto per quelli utilizzati dai governi o dalle agenzie del settore pubblico.

Tuttavia, la sola spiegazione non sarà una panacea. Sebbene la trasparenza sui processi decisionali sia essenziale per la democrazia, sarebbe limitativo pensare che questa rappresenti una facile soluzione ai dilemmi che il processo decisionale algoritmico presenterà sempre più alle nostre società.

---

[65] Cfr. DIANE COYLE, *The tensions between explainable AI and good public policy*. Brookings Institution Press. September 15, 2020 in https://www.brookings.edu/techstream/the-tensions-between-explainable-ai-and-good-public-policy/.

[66] Cfr. ad es. SERGIO GUIDA, *Facial recognition technology is going to be banned in some United States relevant cities*, European Journal of Privacy Law and Technologies, ISSN 2704-8012, 19/05/2019 in http://www.ejplt.tatodpr.eu/Tool/ Evidenza/Single/ view_html?id_evidenza=13 .

[67] Si veda ad es. SERGIO GUIDA, *Per un'Intelligenza Artificiale che ispiri fiducia: la Commissione Europea pubblica le linee -guida sull'etica dell'IA,* Data Protection Law, ISSN 2611-6456, 15/04/2019 in https://www.dataprotectionlaw.it/2019/ 04/15/intelligenza-artificiale-commissione-europea-linee-guida-etica/.

[68] Vedasi *amplius infra*.

Le motivazioni sono due. Innanzitutto, con l'apprendimento automatico in generale e le reti neurali o il *deep learning*[69] in particolare, c'è spesso un compromesso tra prestazioni e spiegabilità, nel senso che più un modello è grande e complesso, più difficile sarà da capire, anche se le sue prestazioni sono generalmente migliori. Sfortunatamente, per situazioni complesse con molte influenze interagenti, il che è vero per molte aree chiave della politica, l'apprendimento automatico più utile sarebbe spesso una scatola nera. Di conseguenza, ritenere tali sistemi responsabili sarà quasi sempre una questione di monitoraggio e valutazione a posteriori. Ad esempio, se si scopre che le decisioni di un determinato algoritmo di apprendimento automatico sono significativamente distorte qualcosa nel sistema o quanto meno i dati su cui è addestrato devono cambiare.

Ci si può ad esempio avvalere di tecniche e strumenti *open source* per rendere maggiormente interpretabili i risultati delle scatole nere dell'AI, con un processo *trial and error* e test di *Explainable AI* per l'interpretazione umana del processo decisionale, finalizzato a correggere eventuali *bias* cognitivi[70], dataset utilizzati per il training e *bug* del modello. Tale da far sì che quest'ultimo possa essere perfezionato apprendendo costantemente dall'essere umano che lo utilizza.

Eppure, anche l'*auditing post hoc* è più facile a dirsi che a farsi. In pratica, il monitoraggio sistematico dei risultati delle politiche è sorprendentemente scarso[71], anche se non mancano indicazioni su come farlo.

---

[69] "Il *deep learning* è un sottoinsieme del *machine learning*, che è essenzialmente una rete neurale con tre o più livelli. Queste reti neurali tentano di simulare il comportamento del cervello umano, anche se lontano dalle sue capacità, permettendogli di "imparare" da grandi quantità di dati. Mentre una rete neurale con un singolo livello può ancora fare previsioni approssimative, ulteriori livelli nascosti possono aiutare a ottimizzare e perfezionare per la precisione.
Il *deep learning* guida molte applicazioni e servizi di intelligenza artificiale (AI) che migliorano l'automazione, eseguendo attività analitiche e fisiche senza l'intervento umano. La tecnologia di *deep learning* è alla base di prodotti e servizi di uso quotidiano (come assistenti digitali, telecomandi TV abilitati alla voce e rilevamento di frodi con carte di credito) nonché di tecnologie emergenti (come le auto a guida autonoma)", come riportato alla pagina web https://www.ibm.com/cloud/learn/deep-learning.

[70] "Un pregiudizio cognitivo descrive un modello replicabile nella distorsione percettiva, nel giudizio impreciso, nell'interpretazione illogica o in quella che viene generalmente chiamata irrazionalità. I pregiudizi cognitivi sono il risultato di distorsioni nella mente umana che portano sempre allo stesso modello di scarso giudizio, spesso innescato da una situazione particolare. Identificare una 'deviazione nel giudizio', richiede uno standard di confronto, cioè 'buon giudizio'. Nelle indagini scientifiche sul *bias* cognitivo, la fonte del 'buon giudizio' è quella di persone al di fuori della situazione ipotizzata per causare il cattivo giudizio, o, se possibile, un insieme di fatti verificabili indipendentemente. L'esistenza della maggior parte dei particolari pregiudizi cognitivi è stata verificata empiricamente in esperimenti di psicologia", come riportato al sito web https://psychology.fandom.com/wiki/List_of_biases_in_judgment_and_decision_making.

[71] Cfr. DIANE COYLE, *The tensions between explainable AI and good public policy*. Brookings Institution Press. September 15, 2020 in https://www.brookings.edu/techstream/the-tensions-between-explainable-ai-and-good-public-policy/, cit..

Il secondo motivo è dovuto a una sfida ancora più significativa. L'obiettivo di molte politiche spesso non viene reso esplicito, in genere perché la politica è emersa come un compromesso tra persone che perseguono obiettivi diversi. Un compromesso nelle politiche pubbliche non è sempre una cosa negativa, consente ai decisori di risolvere i conflitti, ma rappresenta una sfida quando gli algoritmi hanno il compito di implementare le decisioni politiche, in quanto hanno bisogno di obiettivi chiari per funzionare. Un'enfasi su una maggiore spiegabilità del modello non sarà probabilmente in grado di risolvere questa sfida.

Si consideri ad esempio il recente uso di un algoritmo per produrre i voti delle scuole superiori del Regno Unito in assenza di esami durante la pandemia, che fornisce un notevole esempio di quanto male possano funzionare gli algoritmi in assenza di obiettivi ben definiti. Gli insegnanti britannici avevano presentato la loro valutazione dei voti probabili dei singoli alunni e classificato i loro alunni all'interno di ogni materia e classe. L'algoritmo ha declassato significativamente molte migliaia di questi risultati valutati, in particolare nelle scuole statali nelle aree a basso reddito. Quegli alunni con posti universitari condizionati a punteggi molto elevati di conseguenza non sono riusciti a raggiungere il livello di cui avevano bisogno, causando molto dolore, per non parlare del caos nel sistema centralizzato di assegnazione degli studenti alle università. Dopo alcuni giorni di clamore, il governo del Regno Unito ha abbandonato i risultati, assegnando invece a tutti i voti previsti dai loro insegnanti. Quando l'algoritmo è stato finalmente pubblicato, si è scoperto che aveva dato maggior peso alla corrispondenza con la distribuzione dei voti che la stessa scuola aveva ricevuto negli anni precedenti, penalizzando gli alunni migliori delle scuole considerate tipicamente con scarso rendimento. Tuttavia, le classi piccole sono state omesse perché avevano troppe poche osservazioni, il che significava che le scuole private con classi piccole sono sfuggite al declassamento.

Naturalmente, l'intenzione politica non era stata quella di aumentare la disuguaglianza educativa, ma di prevenire l'inflazione di voti alti. Questo obiettivo non era stato dichiarato pubblicamente in anticipo, altrimenti gli statistici avrebbero potuto avvertire delle conseguenze indesiderate. Gli obiettivi di nessuna inflazione di voti, scuola per scuola, e di equità individuale erano fondamentalmente in conflitto. L'ingiustizia nei confronti di alcuni alunni, quelli che avevano lavorato più duramente per superare circostanze sfavorevoli, era inevitabile.

Per le agenzie e gli uffici governativi che fanno sempre più affidamento sull'intelligenza artificiale, il problema principale è che agli algoritmi di apprendimento automatico deve essere assegnato un obiettivo preciso. Eppure, nel mondo disordinato del processo decisionale umano e della politica, è spesso possibile e persino desiderabile evitare di esplicitare obiettivi contrastanti. Bilanciando gli interessi in competizione, il compromesso è essenziale per il sano funzionamento delle democrazie.

Questo è vero anche nel caso di quello che a prima vista potrebbe sembrare un esempio più diretto, come non concedere la libertà su cauzione o vigilata a criminali che potrebbero con alta probabilità essere recidivi. Un algoritmo che utilizza i dati passati per trovare modelli, data la probabilità storicamente più alta che persone appartenenti a comunità a basso reddito o minoranze siano state arrestate o imprigionate, prevede che persone simili hanno maggiori probabilità di offendere in futuro. Forse i giudici potrebbero prestare la massima cautela a questa distorsione dei dati e modificare le indicazioni dell'algoritmo laddove opportuno.

Ma c'è ancora un'ambiguità su ciò che potrebbe essere considerato un buon risultato. Ad esempio, prendere decisioni sulla cauzione: circa un terzo della popolazione carceraria degli Stati Uniti è in attesa di processo. I giudici prendono decisioni ogni giorno su chi attenderà il processo in prigione e chi sarà rilasciato su cauzione, ma un algoritmo può fare una previsione molto più accurata di un essere umano su chi commetterà un reato se viene rilasciato su cauzione. Secondo un modello, se le decisioni sulla cauzione fossero prese da algoritmi, la popolazione carceraria negli Stati Uniti sarebbe del 40% più piccola, con lo stesso tasso di recidiva di quando le decisioni sono prese da esseri umani. Un tale sistema ridurrebbe la popolazione carceraria, con un apparente miglioramento rispetto agli attuali livelli di incarcerazione di massa. Ma dato che le persone di colore costituiscono la grande maggioranza della popolazione carceraria degli Stati Uniti, l'algoritmo potrebbe anche raccomandare che a una percentuale più elevata di persone appartenenti a gruppi di minoranza venga negata la cauzione, il che sembra perpetuare l'ingiustizia.

Alcuni studiosi hanno sostenuto che esporre tali compromessi è una buona cosa. Per gli algoritmi possono quindi essere fissati obiettivi più specifici, ad esempio per prevedere la recidiva soggetta a una regola che richieda la cauzione in proporzioni uguali per soggetti rientranti in gruppi diversi. Inoltre, ciò imporrebbe la trasparenza sugli obiettivi finali.

In Cina, che utilizza sistemi di sorveglianza più intrusivi, è da tempo operativo un meccanismo di credito sociale (simile alla nostra patente di guida a punti) in cui ai cittadini, categorizzati e profilati in base a una raccolta sistematica di big data e all'uso di algoritmi, vengono assegnati o decurtati dei punteggi in funzione della bontà o meno dei loro comportamenti sociali (sulla base di regole definite dal Governo). Lo scopo di tali punteggi è predeterminare il comportamento futuro e allocare risorse e assegnare idoneità per usufruire di servizi pubblici. I cittadini che rispettano le regole ricevono dei premi (sussidi, encomi pubblici), se invece infrangono le regole vengono inseriti in un elenco di persone "interruttori di fiducia" (una *black list* a tutti gli effetti) e possono subire privazioni di diritti e limiti all'accesso ad alcuni benefit o servizi pubblici (sanzioni su sussidi, limiti all'avanzamento di carriera, alla proprietà di beni e alla possibilità di ricevere titoli onorifici dal governo cinese, restrizioni di viaggio in aereo o treni AV).

3. Esperienze nel nostro Paese e garanzie giurisprudenziali.

La necessità nel campo del diritto di confrontarsi con le possibilità tecnologiche offerte dagli incessanti sviluppi dell'IA è parsa procedere con il diffondersi dei software di elaborazione nell'ambito della prassi privata, spaziando dalla concessione del credito all'amministrazione dei sistemi di trading ad alta frequenza di strumenti finanziari, alle scelte in merito alle strategie di marketing più adeguate a raggiungere un determinato mercato *target*, fino a ipotizzare una sorta di "delega in bianco" ai sistemi decisionali automatizzati in merito alla gestione di un contratto tra le parti, attraverso definizione, integrazione, e perfino *enforcement* di uno *smart contract*[72].

Parimenti l'utilizzo di algoritmi a supporto delle decisioni pubbliche si sta diffondendo nella prassi delle amministrazioni ai vari livelli di governo[73].

[72] Cfr. ROBERTO PARDOLESI, ANTONIO DAVOLA, *Algorithmic legal decision making: la fine del mondo (del diritto) o il paese delle meraviglie?* Questione Giustizia n.1/2020 in https://www.questionegiustizia.it/rivista/articolo/algorithmic-legal-decision-making-la-fine-del-mondo-del-diritto-o-il-paese-delle-meraviglie.

[73] Cfr. AGATA QUATTRONE, DEMETRIO NACCARI CARLIZZI, *L'intelligenza artificiale nella Pubblica Amministrazione, un percorso verso il data management*, Ai4business.it, 24 Dicembre 2020 in https://www.ai4business.it/intelligenza-artificiale/lintelligenza-artificiale-nella-pubblica-amministrazione-un-percorso-verso-il-data-management/.

Dal punto di vista operativo, l'AI può diventare la base per una transizione verso il *data management*[74] perché il supporto al processo decisionale grazie alla capacità elaborativa di grandi moli di dati e all'attività predittiva determina un processo di monitoraggio sistematico e selezione delle politiche sulla base dei fatti e conduce, quindi, al *data-driven decision making*[75].

In realtà, però, l'Italia "non solo si trova assente dalla *top ten* dei paesi più avanzati in materia di *eGovernment*, ma si colloca solo al 24° posto (United Nations E-Government Survey 2018)"[76].

A maggior ragione allora, l'IA, già in alcuni casi impiegata per automatizzare e semplificare l'accesso alle informazioni e l'istruzione delle istanze negli enti pubblici, se applicata ai processi organizzativi e decisionali potrebbe risolvere problemi strutturali di efficienza ed efficacia delle procedure amministrative e, apportare significativi benefici alla Pubblica Amministrazione: dalla riduzione eccezionale dei tempi e costi di istruttoria procedimentale al miglioramento delle performance e all'ottimizzazione della gestione delle risorse umane.

Due sentenze del Consiglio di Stato a fine 2019 hanno confermato che la PA può demandare le proprie decisioni a degli algoritmi, soprattutto se queste non dipendono dall'esercizio di un potere discrezionale, ma si fondano su criteri oggettivi e vincolanti. Ci sono però dei principi cardine da rispettare[77].

---

[74] La gestione dei dati "è la pratica di raccogliere, conservare e utilizzare i dati in modo sicuro, efficiente ed economico. L'obiettivo della gestione dei dati è aiutare le persone, le organizzazioni e le cose connesse a ottimizzare l'uso dei dati entro i limiti di policy e normative in modo che possano prendere decisioni e intraprendere azioni che massimizzano il vantaggio per l'organizzazione. Una solida strategia di gestione dei dati sta diventando più importante che mai poiché le organizzazioni fanno sempre più affidamento su risorse immateriali per creare valore", come riportato alla pagina web https://www.oracle.com/database/what-is-data-management/.

[75] "Il processo decisionale guidato dai dati (DDDM) è il processo di utilizzo dei dati per prendere decisioni informate e verificate. I moderni strumenti di analisi come i *dashboard* interattivi aiutano le persone a superare i pregiudizi e a prendere le migliori decisioni manageriali in linea con le strategie", come si legge in BERNARDITA CALZON, *Why Data Driven Decision Making is Your Path To Business Success*, Business Intelligence, Nov 24th 2021 in https://www.datapine.com/blog/data-driven-decision-making-in-businesses/.

[76] Come si legge in LUCIA MUSSELLI, *La decisione amministrativa nell'età degli algoritmi: primi spunti*, Medialaws.it, 2020, in https://www.medialaws.eu/wp-content/uploads/2020/03/1-2020-Musselli.pdf, pag. 22.

[77] Cfr. MASSIMILIANO NICOTRA, *Algoritmi per le decisioni della PA, quali principi seguire: le sentenze*, Agenda Digitale.eu, 09 Gen 2020 in https://www.agendadigitale.eu/sicurezza/algoritmi-per-le-decisioni-della-pa-quali-principi-seguire-le-sentenze/.

Con due sentenze 'gemelle' pubblicate il 13 dicembre 2019 (la n. 2936/2019[78] e la n. 8474/2019[79]) il Consiglio di Stato è tornato sul tema dell'utilizzo di software automatizzati per l'adozione di decisioni di rilievo amministrativo, confermando l'impostazione già assunta nella precedente sentenza 2270/2019 di aprile 2019[80], ma ampliando l'*excursus* argomentativo e scrivendo quello che attenta dottrina ha definito il "vademecum per l'adozione delle decisioni algoritmiche nella pubblica amministrazione"[81].
La vicenda si innesta in un contenzioso che vede contrapposti alcuni dei partecipanti alle procedure per il piano straordinario di assunzioni dei docenti ed il MIUR.
Il Ministero, per dar seguito alla procedura, ha utilizzato un software che, sulla base di parametri e criteri predefiniti, ha provveduto a valutare le domande ed assegnare in maniera automatica le vari sedi a coloro risultati idonei.
Le due sentenze sono particolarmente interessanti e costituiscono il primo vero tentativo da parte della Corte di ultima istanza della giustizia amministrativa di ricostruire in maniera complessiva il fenomeno, dato che, in verità, la precedente pronuncia sopra citata non sembrava aver preso pienamente in considerazione anche gli aspetti inerenti all'applicazione del Regolamento Europeo sulla protezione dei dati personali (GDPR).
Inoltre, i magistrati del Consiglio di Stato si discostano nettamente nel ragionamento, seppur arrivando alle medesime conclusioni, del Tribunale Amministrativo Regionale del Lazio, le cui sentenze erano state oggetto di impugnazioni da parte del MIUR, soprattutto in merito alla legittimità dell'utilizzo di software per decisioni automatizzate nell'ambito dei procedimenti della Pubblica Amministrazione.
Il TAR Lazio aveva escluso la possibilità di utilizzare per l'esercizio dell'attività amministrativa, discrezionale o vincolata, algoritmi informatici per l'assunzione di decisioni automatizzate, sul presupposto che la disciplina del procedimento amministrativo di cui alla Legge 241/1990 ponga in realtà regole e vincoli incompatibili con una piena automazione di tali processi, come ad esempio l'obbligo di individuare un responsabile del procedimento, il diritto di partecipazione da parte del cittadino, l'obbligo di moti-

[78] Il testo è disponibile alla pagina web https://www.tuttocamere.it/files/sentenze/2019_8472_Sent_CdS.pdf.
[79] Testo alla pagina web https://www.tuttocamere.it/files/sentenze/2019_8472_Sent_CdS.pdf.
[80] Il testo è disponibile alla pagina web https://www.lavorodirittieuropa.it/images/Raiti_Consiglio_di_Stato_2270-2019_1.pdf.
[81] Cfr. MASSIMILIANO NICOTRA, Algoritmi per le decisioni della PA, quali principi seguire: le sentenze, Agenda Digitale.eu, 09 Gen 2020 in https://www.agendadigitale.eu/sicurezza/algoritmi-per-le-decisioni-della-pa-quali-principi-seguire-le-sentenze/,cit..

vazione del provvedimento. I giudici amministrativi di primo grado espressamente dichiaravano che "un algoritmo, quantunque preimpostato in guisa da tener conto di posizioni personali, di titoli e punteggi, giammai può assicurare la salvaguardia delle guarentigie procedimentali che gli artt. 2, 6,7,8,9,10 della Legge n. 241/1990 hanno apprestato".

Al contrario, il Consiglio di Stato afferma che anche la PA deve poter sfruttare le rilevanti potenzialità della 'rivoluzione digitale' e che, quindi, il ricorso a tali strumenti, per gli indubbi vantaggi in termini di efficienza ed economicità dell'azione amministrativa (peraltro richiamati dallo stesso art. 1 della Legge n. 241/1990) deve ritenersi pienamente legittimo anche alla luce del principio costituzionale di buon andamento dell'azione amministrativa stabilito dall'art. 97 della Costituzione.

Proprio questo richiamo legittima a livello primario l'utilizzo di tali strumenti e costituisce un'importante affermazione di principio da parte del Consiglio di Stato che:

1. elimina qualsiasi dubbio circa la possibilità che l'amministrazione possa esercitare il proprio potere autoritativo mediante gli stessi
2. chiarisce che in casi analoghi a quello in esame, in cui la discrezionalità amministrativa è vincolata da criteri oggettivi, l'adozione di procedure informatiche che conducano direttamente alla decisione finale deve essere incoraggiata sia per i numerosi vantaggi nello snellimento dell'iter procedimentale sia per le garanzie di maggiore imparzialità che si ottengono.

Non vi sono più dubbi sul fatto che la pubblica amministrazione possa demandare le proprie decisioni a degli algoritmi, soprattutto in quelle ipotesi in cui le decisioni da adottare non dipendono dall'esercizio di un potere discrezionale, ma si fondano su criteri oggettivi e vincolanti per il decisore pubblico. In tal senso l'utilizzo dell'algoritmo diventa uno strumento espressivo dell'agire dell'amministrazione, che può e deve organizzare la propria attività nel rispetto dei principi di efficienza e della trasparenza.

Proprio riprendendo il principio di trasparenza, il Consiglio di Stato indica anche i principi cardine che costituiscono le garanzie minime per ogni ipotesi di utilizzo di algoritmi in sede di decisioni pubbliche sono infatti:

a) la piena conoscibilità;

b) l'imputabilità della decisione.

La piena conoscibilità è riferita ai meccanismi attraverso i quali si concreta la decisione amministrativa, che devono essere pienamente conoscibili *ex ante* in modo da garantire il principio di trasparenza in tutti i suoi aspetti, tanto che, in particolare, esso non può essere limitato da un preteso diritto alla riservatezza delle imprese produttrici del software (cfr. anche *infra*).

In questa direzione le due sentenze richiamate ampliano le argomentazioni rispetto alla precedente pronuncia (la n. 2270/2019): al fine di rimarcare come la norma sovranazionale abbia imposto obblighi informativi a coloro che effettuano trattamenti di dati personali ed abbia riconosciuto un vero e proprio diritto, esercitabile in qualunque momento, in favore degli interessati ad ottenere tali informazioni infatti, il Consiglio di Stato richiama le previsioni del GDPR ed in particolare le norme in materia di informazioni da rendere agli interessati (artt. 13 e 14) e la disciplina del diritto di accesso (art. 15). Evidentemente anche a conferma della rilevanza della trasparenza per i soggetti coinvolti dall'attività amministrativa informatizzata.

Più in generale, il principio di trasparenza trova ormai diretta applicazione anche in conseguenza della previsione ex art. 5, 1° comma, lett. a) del GDPR, che nel formalizzare tale principio ha inoltre assoggettato le violazioni dello stesso alla sanzione pecuniaria più alta prevista.

L'imputabilità è direttamente correlata alla responsabilità della Pa, visto che *"l' autonomia (dell'algoritmo, ndr) è di natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente; (...) nell'ipotesi in cui un robot possa prendere decisioni autonome, le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati» (Carta Robotica Parlamento Ue)*[82]*. Insomma, specifica il giudice amministrativo, "deve essere garantita l'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile, sia nell'interesse della stessa p.a. che dei soggetti coinvolti ed incisi dall'azione amministrativa affidata all'algoritmo".*

[82] È la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), P8_TA-PROV (2017)0051 in https://www.altalex.com/documents/leggi/2017/02/20/norme-di-diritto-civile-sulla-robotica.

Il fondamento del principio di imputabilità risiede quindi nella necessità di garantire la verifica, in termini di logicità e correttezza, degli esiti delle decisioni automatizzate: è necessario, quindi, che sia individuato un soggetto responsabile a cui possano essere ricondotti gli effetti dell'azione amministrativa adottata dall'algoritmo.

Il Consiglio di Stato richiama l'art. 22 del GDPR, che disciplina proprio il procedimento automatizzato del trattamento dei dati personali ai fini di una decisione amministrativa e prevede che: *"l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona."* Questo principio trova la sua corrispondenza nel 15simo "Considerando" del GDPR, laddove è previsto che *"al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche (il trattamento) dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate"*. "*Entrambe le previsioni sono perciò perfettamente coerenti con i principi fissati dal diritto amministrativo domestico che in sede di coordinamento tra regole sulla trasparenza ed esigenza di rispetto della normativa sulla protezione dei dati si coniugano da un lato con la discrezionalità amministrativa, dall'altro con la categoria dell'atto vincolato alle quali tutte le amministrazioni pubbliche sono sottoposte e che pone, alla nostra attenzione, ulteriori profili di criticità in ordine all'algoritmo assunto alla base di una decisione adottata dal sistema di intelligenza artificiale*"[83].

Il primo profilo riguarda la necessità di rispettare il principio di trasparenza, che ormai è centrale nell'attività della P.A. e dovrà essere alla base dei nuovi servizi pubblici fondati su algoritmi e decisioni automatizzate: in tal senso, occorrerà assicurare la trasparenza non solo dei dati, ma anche degli algoritmi, delle logiche di costruzione dei *database*, del processo di funzionamento del servizio.

Il secondo attiene alla responsabilità giuridica della Pubblica Amministrazione anche quando ricorre a soluzioni IA nell'erogazione dei servizi o a procedimenti interamente automatizzati. La giurisprudenza amministrativa si è occupata di casi in cui il procedimento amministrativo è governato completamente da una macchina e si è mossa tenendo fermo il presupposto fondamentale, quello cioè che la tutela giurisdizionale non può essere esclusa o limitata per determinate categorie di atti.

[83] Cfr. MICHELE GORGA, *Privacy e processo decisionale automatizzato nella PA*, 26 dicembre 2020 in https://www. Prp channel.com/privacy-e-processo-decisionale-automatizzato-nella-pa/.

Con una sentenza del 2 gennaio 2020[84] il Consiglio di Stato si è poi *"soffermato sul ruolo di controinteressato rivestito dal produttore dell'algoritmo e i diritti connessi, issando un principio destinato a rimanere un cardine nel contenzioso inerente software e algoritmi, in particolare quando essi vengano utilizzati nell'ambito di procedimenti e concorsi pubblici"*[85].

La sentenza è stata resa nell'ambito di un contenzioso tra il MIUR, un gruppo di concorrenti del *"Corso-concorso nazionale, per titoli ed esami, finalizzato al reclutamento di dirigenti scolastici presso le istituzioni scolastiche statali"* e il Cineca – Consorzio Interuniversitario: gli aspiranti hanno partecipato al concorso in questione ed affrontato la prova scritta con esito negativo, ritenendo che ciò sia dipeso da un funzionamento del software che gestiva la prova diverso rispetto alle indicazioni fornite dal Ministero con un apposito tutorial diramato sul sito web della stessa Amministrazione statale.

In particolare, *"secondo le contestazioni dei candidati, il software non avrebbe previsto la funzione di salvataggio automatico delle risposte rese, né la necessità di procedere ad un salvataggio manuale delle risposte fornite ai quesiti; nessuna funzione, inoltre, sarebbe stata enucleabile dalla tastiera del computer, non annoverante un apposito pulsante con la dicitura "salva"; nel corso delle operazioni, in taluni casi, si sarebbe verificato altresì il blocco del sistema prima della fine del tempo a disposizione per terminare la prova. Pertanto, è stata presentata nel gennaio 2019 una richiesta di accesso comprendente l'algoritmo di calcolo e i codici sorgente che hanno gestito il software relativo alla prova scritta, al fine di accertare la causa delle irregolarità riscontrate. Il Ministero non aveva consentito l'accesso, così i candidati presentavano ricorso al Tar Roma, chiedendo l'accertamento del proprio diritto ad accedere e prendere visione del codice sorgente, ovvero dell'algoritmo di calcolo del software che ha gestito le prove scritte del concorso in parola e del programma utilizzato in occasione della prova svoltasi in data 18 ottobre 2018. Il Tar accoglieva il*

[84] La sentenza del Consiglio di Stato è la n. 30 del 2 gennaio 2020, il testo è disponibile in https://www.segretaricomunalivighenzi.it/ archivio/2020/gennaio/09-01-2020-il-controinteressato-nel-laccesso-agli-atti-nel-procedimento-e-nel-processo.

[85] Cfr. ELIO ERRICHIELLO, *Algoritmi nella PA: accesso al software e diritti del produttore, i paletti del Consiglio di Stato.* Agendadigitale.eu (ISSN 2421-4167), 5 Febbraio 2020 in https://www.agendadigitale.eu/documenti/algoritmi-nella-pa-accesso-al-software-e-diritti-del-produttore-i-paletti-del-consiglio-di-stato/.

ricorso, statuendo, tra l'altro, che il Cineca (autore del software) non fosse tecnicamente qualificabile come controinteressato. Il Miur presentava appello contro la sentenza"[86].

Il Consiglio di Stato, partendo dalle nozioni generali del procedimento amministrativo, fissa, come evidenziato dall'autorevole commentatore, un principio cardine nel contenzioso inerente software e algoritmi.

In particolare, *"secondo la Giustizia amministrativa, l'ostensione del codice sorgente procurerebbe un grave pregiudizio sia alle esigenze di riservatezza della procedura concorsuale (rilevando le formule e le istruzioni occorrenti per decriptare e gestire quesiti e risposte, nonché tutti i dati inseriti dai candidati del concorso, con conseguente violazione della riservatezza e della regolarità delle operazioni concorsuali), sia al diritto di riservatezza riconoscibile al titolare dello stesso algoritmo, rendendo note tutte le parti di ideazione e strutturazione del software, oggetto di protezione alla stregua del diritto di proprietà intellettuale e industriale; fattispecie limitative del diritto di accesso ai sensi degli artt. 24, comma 6, lett. d), L. n. 241/90, 5 bis, comma 2, lett. c) D. Lgs. n. 33/2013 e 53, comma 5, lett. d), D. Lgs. n. 50/2016. Sulla base di queste considerazioni, con la sentenza in commento il Collegio ha disposto l'annullamento della sentenza appellata e la rimessione della causa al Tar in maniera che il processo possa celebrarsi, fin dal primo grado di giudizio, nel contraddittorio con il Cineca"*[87].

Come evidenziato, *"la sentenza da una parte assume una piega garantista nei confronti delle società informatiche, che avranno diritto a essere coinvolte nei procedimenti amministrativi di accesso, d'altro canto pare anticipare che il diritto di accesso – che quando diretto a consentire la tutela in giudizio dei propri diritti e interessi legittimi secondo un orientamento pacifico supera il diritto alla riservatezza – possa invece trovare uno specifico ostacolo in tema di software, dove consentire l'accesso al codice sorgente potrebbe comportare un grave danno economico per il terzo oltre che svelare l'intero iter concorsuale. Nella pur difficile ricerca di equilibrio necessario tra diritto di accesso e tutela della riservatezza, sarà fondamentale che la giuri-*

[86] *Ibidem*.
[87] *Ibidem*.

sprudenza individui un giusto bilanciamento per evitare che le esigenze e le prerogative economiche (legate alla proprietà intellettuale del software) divengano un ostacolo alla tutela dei propri diritti in giudizio"[88].

Guardando verso il futuro, va riconosciuto che le esperienze di applicazione di soluzioni IA maturate nella PA, nella stragrande maggioranza dei casi, sono state ben inquadrate dalla giurisprudenza laddove erano intervenute per automatizzare in maniera tracciabile iter procedimentali interni a bassa complessità e alto costo, standard e routinari, senza invadere il campo delle scelte discrezionali.

Altre soluzioni di AI più complesse, in cui è lo sviluppatore a implementare le regole decisionali, utilizzano l'apprendimento automatico (*Machine Learning, ut supra*) per identificare schemi ricorrenti e, su questa base, assumere una decisione o fare una previsione. È logico prevedere che l'utilizzo di sistemi di apprendimento automatico supervisionato, anche con un tasso medio di successo elevato, determini consensi diversi a seconda dell'interesse in gioco e del bene tutelato. In questo caso il problema può nascere in relazione alla presenza di più interessi da tutelare, quando le istruzioni per il loro contemperamento rimangano insufficienti o indeterminate.

E, infine, ci sono i più sofisticati sistemi di intelligenza artificiale che usano reti neurali profonde che possono auto-apprendere, anche senza la supervisione umana. Il *Deep Learning* (*ut supra*) negli ultimi anni ha consentito l'implementazione di algoritmi che risolvono problemi che il *Machine Learning* e altre tradizionali tecniche di AI non consentivano o per i quali il margine di errore nelle predizioni era ancora significativamente elevato. Ciò al prezzo di una considerevole perdita in termini di trasparenza, controllo e tracciabilità.

Le reti neurali profonde non permettono, infatti, una piena "interpretabilità" (*explainability*) del processo decisionale attraverso il quale i sistemi *Deep Learning* arrivano a una decisione specifica e quindi di comprendere quali fattori o dati siano stati decisivi nella produzione di un determinato risultato. In questi casi si pone la questione cruciale e tuttora aperta della "*AI black box*"[89] (la scatola nera dell'intelligenza artificiale, cfr. *supra*).

---

[88] *Ibidem*.

[89] Cfr. "Fondamentalmente, le scatole nere sono algoritmi che gli esseri umani non possono rilevare, cioè sono sistemi epistemicamente opachi che nessun essere umano o gruppo di umani può esaminare da vicino per determinare i suoi stati interni. In genere, un algoritmo *black box* non segue regole ben comprese (come, ad esempio, fa un algoritmo *Boolean Decision Rules*), ma può essere "addestrato" con dati etichettati per riconoscere schemi o relazioni nei dati, e come tale può classificare nuovi dati. (…) Tali sistemi sono tipicamente fatti con migliaia di punti dati. La loro accuratezza, al contrario, viene

Il procedimento amministrativo così come lo conosciamo, tramite i suoi principi, tutela il cittadino dall'Autorità. Tale tutela diventa rischio di fronte alla mancata trasparenza e conoscibilità delle *AI black box*. Si interromperebbe un lungo cammino che oggi, tramite accesso e partecipazione al procedimento, apertura dei dati, trasparenza totale anche grazie al digitale sta conducendo verso un modello di democrazia più matura e deliberativa.

Il problema di una decisione "al buio" pone poi anche un problema di assenza di un controllo antropocentrico[90] e quindi della legittimazione democratico-elettiva della decisione pubblica. Ed è anche un problema sostanziale rispetto all'incertezza circa la capacità degli algoritmi di *Deep Learning* di generare di per sé un'adeguata affidabilità interpretativa semantica[91].

È certamente vero che la quotidianità ci ha abituato a errori sintattici e semantici anche evidenti nell'attività decisionale umana in tutti i campi compresa la PA. Ma l'errore umano è leggibile e "giustiziabile" proprio alla stregua dei parametri di ragionevolezza e corrispondenza ai canoni del diritto, in quanto ristretto in percorsi e provvedimenti limitati ed intellegibili quantitativamente.

La PA è quindi un terreno scivoloso proprio per il necessario contemperamento di diversi interessi potenzialmente conflittuali. È più facile accettare errori nel *policy making* tradizionale che esiti di decisioni assunte sulla base della attività non trasparente o evidente del *Deep Learning*. Ciò aggrava il problema di obiettivi ed istruzioni chiari e determinati per gli algoritmi e di una loro evoluzione nella capacità semantica.

Ora è necessario tornare ancora una volta al più volte richiamato articolo 22 del GDPR, che ha fissato una regola di tutela secondo la quale l'interessato al trattamento dei dati

---

testata rispetto a un diverso insieme di punti dati di cui è nota l'etichettatura (cioè eseguita da esseri umani). È interessante notare che, anche se si pretende di comprendere i principi matematici che governano l'algoritmo, è ancora complicato e spesso persino impossibile pretendere di comprendere il funzionamento interno di tali sistemi. (..) L'opacità epistemologica che caratterizza gli algoritmi *black box* sembra essere in conflitto con gran parte della pratica discorsiva del dare e chiedere ragioni per credere ai risultati di un algoritmo, che sono alla base della descrizione della responsabilità morale. Le preoccupazioni riguardano problemi di responsabilità e trasparenza con l'uso di questi algoritmi, discriminazione (nascosta) e pregiudizi che emergono da algoritmi opachi e l'aumento di risultati incerti che potenzialmente minano l'autorità epistemica degli esperti che utilizzano algoritmi *black box*" in JUAN MANUEL DURÁN, KARIN ROLANDA JONGSMA, *Who is afraid of black box algorithms? On the epistemological and ethical basis of trust in medical AI*, Journal of Medical Ethics, 18 March 2021 in http://dx.doi.org/10.1136/medethics-2020-106820, pag.329.

[90] Cfr. AGATA QUATTRONE, DEMETRIO NACCARI CARLIZZI, *L'intelligenza artificiale nella Pubblica Amministrazione, un percorso verso il data management*, Ai4business.it, 24 Dicembre 2020 in https://www.ai4business.it/intelligenza-artificiale/lintelligenza-artificiale-nella-pubblica-amministrazione-un-percorso-verso-il-data-management/, cit..

[91] *Ibidem.*

ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Ha diritto quindi a che le decisioni che lo riguardano non siano basate esclusivamente sulla decisione algoritmica, fatte salve alcune eccezioni.

Su tale regola si innesta il principio fissato dal Consiglio di Stato nella sentenza 8472/2020[92] che ha sancito appunto il principio della non esclusività della decisione algoritmica. Vale a dire il diritto a un processo decisionale dove la valutazione umana abbia un ruolo, avendo ognuno il diritto a che tale decisione non sia basata unicamente su tale processo automatizzato (art. 22 GDPR). In proposito, deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informativo il modello viene definito come HITL (*human in the loop*)[93], in cui per produrre il suo risultato è necessario che la macchina interagisca con l'essere umano.

Anche in dottrina qualche studioso ha parlato di una *"concezione antropocentrica dell'amministrazione 4.0.: tale soluzione propone di assicurare un ruolo comunque centrale del funzionario nelle decisioni automatizzate, garantendo ad esso uno spatium deliberandi in merito al prodotto dell'algoritmo ed evitando una completa deresponsabilizzazione"*[94]. Secondo altri, "*il primo e più importante principio generale è quello che, allorquando si applichino processi di automatizzazione nel contesto del settore pubblico, deve sempre essere garantita la supervisione dei risultati da parte di un 'funzionario persona fisica'. A parere di chi scrive non è cioè immaginabile sostituire con un algoritmo la figura del funzionario responsabile del procedimento: piuttosto, è viceversa certamente possibile immaginare che il funzionario responsabile del*

[92] Testo disponibile alla pagina web https://www.lavoripubblici.it/documenti2021/lvpb1/sentenza-cds-29.12.2020-8472.pdf.

[93] "*Human In The Loop (HITL)* è tradizionalmente definito come "un modello che richiede l'interazione umana". In un contesto di *Machine Learning*, implica un modello di calcolo ibrido in cui un essere umano può intervenire per annullare le decisioni prese da una macchina in cui è meno probabile che siano corrette. Ciò è determinato dalla fiducia della macchina in ogni decisione che prende. (..) Il punto del modello HITL è sfruttare i vantaggi di riduzione dei costi dell'automazione - attraverso algoritmi, modelli statistici, intelligenza artificiale, lo chiami - mitigando i potenziali errori facendo in modo che le persone si occupino di situazioni difficili. Questo conta tanto più quanto maggiore è il costo di un errore. Tuttavia, rimuovere la supervisione umana su determinati tipi di decisioni algoritmiche, quelle ad alta confidenza, può generare rischi nascosti poiché le condizioni dell'ambiente in cui opera l'algoritmo cambiano", come si legge in BERNAT FAGES, *Introduction to Human In The Loop*, April 30, 2020 in https://www.humanlambdas.com/post/an-introduction-to-human-in-the-loop.

[94] Cfr. FABIO ANSELMI, *L'algoritmizzazione della Pubblica Amministrazione: le prospettive per una PA 4.0*, Lexacivis.com, 07/04/21 in https://lexacivis.com/2021/04/07/lalgoritmizzazione-della-pubblica-amministrazione-le-prospettive-per-una-pa-4-0/.

procedimento si serva utilmente dell'IA per poter svolgere più rapidamente, e con maggiore precisione, attività della fase istruttoria delle quali resta, ovviamente, il responsabile: sia in termini di verifica dei risultati della stessa, sia in termini di collegamento fra le risultanze della fase istruttoria e l'adozione della decisione finale che confluisce nel provvedimento conclusivo del procedimento"[95].

A questo punto, si può dedurre che, mentre sono certamente ammissibili algoritmi di ausilio all'attività amministrativa che supportano le decisioni umane dell'amministrazione, operando un supporto quantitativo nella elaborazione di dati e processando istruzioni umane, non risultano ancora compatibili col nostro diritto amministrativo decisioni autonome dell'AI, fondate su algoritmi di *deep learning*, dove (come abbiamo visto anche *supra*) la scelta si fonda su un percorso logico non ricostruibile e dove esiste una discrezionalità della scelta che viene di fatto rimessa in capo alle valutazioni dell' IA, non evidenti per l'uomo.

Il problema della diffusione di algoritmi evoluti di AI e *deep learning* è quindi più che mai aperto sugli aspetti di *accountability* dell'algoritmo che risultano decisivi nella valutazione di compatibilità amministrativa, cioè:

1. trasparenza della decisione come possibilità di verificare la sequenza delle valutazioni e delle istruzioni applicate alla mole di informazioni che determinano il risultato finale al fine di consentire il sindacato di legittimità della scelta.
2. imputazione della decisione anche nella dimensione dell'apprezzamento di merito della scelta nel circuito democratico.

Se lo schema della scelta autoritativa nel nostro ordinamento si fonda sulla evidenza della sequenza logica di decisione, attribuire il potere di scelta ad una elaborazione non ricostruibile fa venire meno la legittimazione democratica del potere stesso di scelta. Tutto ciò cancella il diritto alla partecipazione al procedimento amministrativo come elemento del diritto di cittadinanza. Ciò impedisce la tutela degli interessi pubblici e privati, poiché senza evidenza del processo decisionale verrebbero meno gli elementi cardine della tutela dell'interesse legittimo: l'obbligo di motivazione e la sua ragionevolezza.

[95] Cfr. DIANA-URANIA GALETTA, JUAN GUSTAVO CORVALÁN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in Federalismi.it (http://www.federalismi.it), Numero 3/2019, 6 febbraio 2019, pp. 1-23, in https://air.unimi.it/retrieve/handle/2434/623522/1367409/GalettaCorvalan DecisioneAlgoritmica2019OpenAccess.pdf, pag.18.

Il motivo per cui non è secondaria tale investigazione-evoluzione sta nel significato storico della procedimentalizzazione dell'azione amministrativa quale tentativo di dare forma giuridica definita all'esercizio dell'autorità. In Europa il primato della legge nasce come limite dell'esecutivo, attraverso la creazione di regole poste nell'interesse generale e la codificazione di atti tipici attraverso i quali ridurre l'arbitrio del potere esecutivo.

Il risultato è stata la progressiva riduzione della discrezionalità amministrativa e la crescente ammissione di spazi di tutela degli interessi del privato verso la PA. Il procedimento amministrativo nasce quindi come garanzia per arginare il potere assoluto e si sviluppa in una funzione garantista.

La ricerca di una teoria del procedimento amministrativo digitale e algoritmico che non stravolga i valori e i parametri del procedimento amministrativo nativo umano è lo scenario dell'implementazione delle tecnologie digitali e dell'Agenda Digitale come settore che sta ormai sostituendosi alla tradizionale corrente di riforma della PA.

Muovendo da tale consapevolezza il Codice dell'amministrazione digitale impone alle amministrazioni di organizzare autonomamente la propria attività facendo ricorso alle tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di *"efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione"*. *"In questa prospettiva, si è parlato di 'nuova rivoluzione industriale' tenuto conto degli innovativi scenari sul piano sia tecnico produttivo che socioeconomico, che pongono problemi di mediazione giuridica e di responsabilità"*[96].

Secondo tale dottrina, *"la relazione tra intelligenze artificiali e amministrazioni pubbliche nello svolgimento di attività e nell'assunzione di decisioni connotate da diversi gradi di discrezionalità appare offrire al momento tre strade o possibili modelli alternativi di riferimento"*[97].

1) Un primo modello, 'preclusivo e divisivo': rivendica i caratteri tipici della discrezionalità amministrativa come categoria giuridica della libertà ed espressione della

[96] Cfr. BIANCAMARIA RAGANELLI, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenza diverse nell'assunzione di decisioni amministrative*. ISSN 1826-3534 Federalismi. federalismi.it – ISSN 1826-3534. N.22 -22 Luglio 2020 in https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=43866, pdf in https://www.federalismi.it/ ApplOpenFilePDF.cfm?artid=43866&dpath=document&dfile=22072020081149.pdf&content=Decisioni%2Bpubbliche%2Be%2Balgoritmi%3A%2Bmodelli%2Bdi%2Bdialogo%2Bnell%27assunzione%2Bdi%2Bdecisioni%2Bamministrative%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, pag. 244.

[97] *Ibidem*, pag. 258.

volontà dell'amministrazione, che dovrebbe restare per assunto preclusa allo "straniero", inteso come tutto ciò che è "altro" rispetto a quanto fino ad oggi abbiamo ritenuto debba essere. Una sorta di dualismo per separazione, (..) che può naturalmente poi trovare declinazioni diverse in base alla maggiore o minore rigidità nel definire e fissare la soglia o ampiezza della discrezionalità, che, come noto, è elemento costitutivo dell'attività amministrativa complessivamente considerata, così potendo finire per escludere completamente il ricorso agli algoritmi c.d. intelligenti dall'attività amministrativa connotata da una sia pur minima parvenza di discrezionalità. Dipende ancora una volta dai parametri di riferimento a seconda che si guardi alla c.d. "neutralità" della pubblica amministrazione (artt. 97 e 98 Cost.), rispetto alla quale può parlarsi di "merito amministrativo" ovvero di "opportunità amministrativa", ovvero alla volontà politica, che si esprime negli atti di indirizzo, di coordinamento, di direzione e continua ad essere ritenuta libera nel fine e da forme di controllo, salvo un controllo esterno e "in negativo" sui limiti del potere esercitato, sul c.d. *abuse of power*.

2) Un secondo modello, 'di tipo cooperativo': guarda invece alle IA come valido strumento di supporto istruttorio per il decisore-funzionario-essere umano, quale strumento di ricerca, semplificazione e selezione delle diverse ipotesi decisorie, con i relativi pro e contra, ad ausilio dell'attività intellettiva umana di ponderazione dei diversi interessi compresenti nell'obiettivo di pervenire alla miglior scelta provvedimentale. Questo modello riconosce l'endiadi "uomo-macchina": la matematica e la tecnologia sono poste a supporto dell'attività amministrativa tradizionalmente intesa, così escludendo le ipotesi futuristiche ispirate alla figura del "funzionario-robot". Ciò risulta compatibile con l'impostazione secondo cui nell'agire discrezionale è sempre presente un minimo di "politicità" della decisione, che si giustifica unicamente in ragione della legittimazione democratica degli apparati amministrativi, i cui organi intesi in senso tradizionale sono riconducibili al circuito democratico-rappresentativo. Tale impostazione consentirebbe inoltre di superare il complesso tema dell'imputazione formale dell'atto amministrativo a integrale elaborazione elettronica, il quale richiederebbe altrimenti di confrontarsi con il più ampio tema della soggettività giuridica degli elaboratori elettronici. Questa prospettiva risulta in linea con il regolamento Ue 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla

libera circolazione di tali dati. Questo richiama il diritto dell'interessato a non essere sottoposto a decisioni basate unicamente sul *trattamento automatizzato* e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona". Sul punto il Consiglio di Stato nel 2020 ha enucleato il principio della non esclusività della decisione algoritmica", cfr. *supra*.

3) Secondo un terzo modello, 'di *autoregolazione*', le intelligenze artificiali potrebbero spingersi oltre il confine dell'agire amministrativo discrezionale laddove si intendesse valorizzare sul piano giuridico il potere di "autolimitazione" della pubblica amministrazione, quale espressione della rispettiva sfera di autonomia organizzativa e funzionale. (..) Predeterminando a priori la propria azione futura e vincolandosi a specifiche regole per scelta propria e connessa assunzione di responsabilità per i successivi atti, anche se automatizzati, l'amministrazione potrebbe declinare gli spazi di discrezionalità del potere, così da consentirne la traduzione in precise istruzioni e algoritmi. (…) Ad oggi, il modello risulta potenzialmente applicabile a specifici procedimenti amministrativi di attribuzione di vantaggi economici, dove le scelte amministrative sono inquadrabili entro le griglie di parametri specifici preventivamente resi pubblici dall'amministrazione procedente. Permangono tuttavia forti difficoltà a estenderlo ad altri settori[98].

4. Conclusioni.

Le problematiche emergenti coinvolgono il tema del rapporto, complicato, tra diritto e tecnologia. *"Quanto può il diritto cristallizzare la tecnologia? Sembra esserci un problema di fondo: la norma non può codificare un qualcosa che è soggetto ad una rapidissima capacità di cambiamento e trasformazione. L'evoluzione avviene ad una velocità tale che le norme scritte diventano obsolete nel giro di pochi anni. Di conseguenza, una norma rigida e specifica risulterebbe in breve tempo inapplicabile, quantomeno non nei termini di dettaglio con i quali il legislatore l'aveva scritta. Questo fa sempre più pensare che la transizione digitale della pubblica amministrazione non comporti solamente un ripensamento dell'azione e dell'organizzazione amministrativa, ma coinvolga gli stessi principi fondanti il diritto amministrativo, fino a ipotizzare una reinterpretazione della tradizionale dialettica autorità-libertà"*[99].

[98] *Ibidem*, pagg. 259-260.
[99] Cfr. FABIO ANSELMI, *L'algoritmizzazione della Pubblica Amministrazione: le prospettive per una PA 4.0*, Lexacivis.com, 07/04/21 in https://lexacivis.com/2021/04/07/lalgoritmizzazione-della-pubblica-amministrazione-le-prospettive-per-una-pa-4-0/, cit..

Ma c'è di più: *"una marcata e decisiva relazione tra implementazione di sistemi di AI e vita buona dell'essere umano. Questo principio viene così esplicitato: 'lo sviluppo dell'IA deve essere incentrato sull'inclusione economica e sociale, sui diritti umani e sulla sostenibilità ambientale. L'IA deve essere progettata e implementata in modo responsabile e trasparente, affinché possa rispondere alle sfide della società garantendo sicurezza in tutti i settori' (2.2 punto 3). È la via europea che viene dichiarata come la via italiana: la via antropocentrica. Potremmo a buon diritto dire anche il viceversa, nel senso che la cultura italiana su questi temi è elemento fondante della cultura europea grazie al processo osmotico tra i nostri valori costituzionali e quelli dei trattati dell'Unione che si sono susseguiti nel tempo"*[100].

In realtà, a mio avviso la posta in gioco è ancora più elevata, se proprio pochi giorni fa l'Unesco ha ritenuto di adottare una 'Raccomandazione' contro i rischi degli algoritmi sui diritti sociali: Audrey Azoulay, Direttore Generale dell'UNESCO, ha presentato a fine novembre il primo standard globale sull'etica dell'intelligenza artificiale adottato dagli Stati membri dell'UNESCO alla Conferenza Generale[101]: *"questo testo storico definisce i valori e i principi comuni che guideranno la costruzione dell'infrastruttura legale necessaria per garantire il sano sviluppo dell'IA. L'intelligenza artificiale è pervasiva e consente molte delle nostre routine quotidiane: prenotazione di voli, guida di auto senza conducente e personalizzazione dei nostri feed di notizie mattutine. L'IA supporta anche il processo decisionale dei governi e del settore privato. (..) Ma la tecnologia sta portando anche nuove sfide senza precedenti. Vediamo un aumento del pregiudizio di genere ed etnico, minacce significative alla privacy, alla dignità e al concetto di agency, pericoli della sorveglianza di massa e un maggiore uso di tecnologie di intelligenza artificiale inaffidabili nelle forze dell'ordine, solo per citarne alcuni. Finora non esistevano standard universali per fornire una risposta a questi problemi".*

E ancora *"il mondo ha bisogno di regole per l'intelligenza artificiale a beneficio dell'umanità. La Raccomandazione sull'etica dell'IA è una risposta importante. Sta-*

[100] Cfr. LUCA PEYRON, *Intelligenza Artificiale: l'Italia lancia la strategia nazionale*, HuffPost 02/12/2021 in https://www. huffingtonpost.it/ entry/intelligenza-artificiale-litalia-lancia-la-strategia-nazionale_it_61a8d9b8e4b0451e551243df?utm_hp_ref=it-homepage.

[101] Cfr. UNESCO *member states adopt the first ever global agreement on the Ethics of Artificial Intelligence*, Press release 25/11/2021, in https://en.unesco.org/news/unesco-member-states-adopt-first-ever-global-agreement-ethics-artificial-intelligence.

bilisce il primo quadro normativo globale dando agli Stati la responsabilità di applicarlo al loro livello. L'UNESCO sosterrà i suoi 193 Stati membri nella sua attuazione e chiederà loro di riferire regolarmente sui loro progressi e pratiche".

La raccomandazione mira a realizzare i vantaggi che l'IA porta alla società e a ridurre i rischi che comporta, per assicurare che le trasformazioni digitali promuovano i diritti umani e contribuiscano al raggiungimento degli obiettivi di sviluppo sostenibile, affrontando questioni relative a trasparenza, responsabilità e privacy.

In particolare, la raccomandazione vieta esplicitamente l'uso di sistemi di intelligenza artificiale per il punteggio sociale e la sorveglianza di massa, visto che questi tipi di tecnologie sono molto invasive, violano i diritti umani e le libertà fondamentali e vengono utilizzate in modo ampio. La raccomandazione sottolinea anche che quando sviluppano quadri normativi, gli Stati membri dovrebbero considerare che la responsabilità ultima deve sempre spettare agli esseri umani e che le tecnologie di intelligenza artificiale non dovrebbero essere dotate di personalità giuridica.

Il 30 novembre 2021, *European Digital Rights* (EDRi) e 119 organizzazioni della società civile hanno lanciato una dichiarazione collettiva per chiedere un Atto sull'Intelligenza Artificiale (AIA) che metta in primo piano i diritti fondamentali.

La dichiarazione delinea le raccomandazioni centrali per guidare il Parlamento europeo e il Consiglio dell'Unione europea nella modifica della proposta AIA della Commissione europea[102].

---

[102] Come visto anche *supra*, il 21 aprile 2021, la Commissione Europea ha pubblicato una proposta legislativa per un *Artificial Intelligence Act (AI Act)*. La legge sull'IA affronta i rischi dei sistemi di IA per la sicurezza o i diritti fondamentali dei cittadini seguendo un approccio basato su rischi che vanno dall'inaccettabile al minimo. Mentre alcune pratiche dannose abilitate all'IA sarebbero completamente vietate, i sistemi di IA ad alto rischio sarebbero soggetti a requisiti obbligatori. (..)

Definizione di AI: lun sistema di intelligenza artificiale viene definito come "software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I e in grado, per un determinato insieme di obiettivi definiti dall'uomo, di generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono". (Atto AI art. 3). Gli approcci elencati nell'allegato sono approcci di apprendimento automatico, approcci basati sulla logica e sulla conoscenza e approcci statistici. L'elenco può essere adattato dalla Commissione europea per coprire il nuovo mercato e gli sviluppi tecnologici. (Articolo 4.)

Regolamento basato sul rischio – Rischio inaccettabile: l'*AI Act* utilizzerebbe un approccio basato sul rischio con quattro livelli di rischio: rischio inaccettabile, rischio alto, rischio limitato e rischio minimo/nessun rischio. Alcuni sistemi di intelligenza artificiale che causano o potrebbero causare un danno fisico o psicologico a una persona sarebbero completamente vietati. Non sarebbe consentito immettere sul mercato, mettere in servizio o utilizzare i seguenti sistemi di IA:

- che implementano tecniche subliminali oltre la coscienza di una persona
- che sfruttano le vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità fisica o mentale
- che forniscono un punteggio sociale alle persone fisiche per un certo periodo di tempo per scopi generali che portino a un trattamento dannoso o sfavorevole

I firmatari chiedono[103]:

- ✓ *Un approccio coerente, flessibile e a prova di futuro al "rischio" dei sistemi di IA.* Compreso un meccanismo solido e coerente per aggiornare i sistemi di IA che rientrano nelle categorie di rischio "inaccettabile" (articolo 5) e garantire che anche i titoli dei settori "ad alto rischio" (allegato III) possano essere aggiornati.
- ✓ *Divieti su tutti i sistemi di IA che presentano un rischio inaccettabile per i diritti fondamentali.*

  Compreso il divieto totale di: sistemi di punteggio sociale; identificazione biometrica remota in spazi pubblicamente accessibili (da tutti gli attori); sistemi di riconoscimento delle emozioni; categorizzazione biometrica discriminatoria; fisiognomica IA; sistemi utilizzati per prevedere future attività criminali; sistemi per profilare e valutare il rischio in un contesto migratorio.
- ✓ *Obblighi degli utenti di (ovvero coloro che implementano) sistemi di IA ad alto rischio per facilitare la responsabilità nei confronti di coloro che sono colpiti da tali sistemi.*

- ➢ di identificazione biometrica remota in tempo reale utilizzati negli spazi pubblicamente accessibili dalle forze dell'ordine, con alcune limitate eccezioni (art. 5, comma 1.) Quando si applica un'eccezione per l'uso di sistemi di identificazione biometrica remota in tempo reale da parte delle forze dell'ordine, i sistemi dovrebbero rispettare garanzie aggiuntive, come la necessità, la proporzionalità e l'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente. (art. 5, cpv. 2-4.).

Sistemi di intelligenza artificiale ad alto rischio: i sistemi di IA destinati all'uso come componenti di sicurezza di prodotti soggetti a valutazione della conformità ex ante da parte di terzi e i sistemi di IA autonomi che hanno implicazioni per i diritti fondamentali e sono esplicitamente elencati nell'allegato III della legge sull'IA sarebbero classificati a rischio elevato. (Art. 6.) (..) I sistemi di IA ad alto rischio sarebbero soggetti a requisiti obbligatori relativi alla qualità dei set di dati utilizzati; documentazione tecnica; tenuta dei registri; trasparenza e informativa agli utenti; supervisione umana; e robustezza, accuratezza e sicurezza informatica. (Articoli 8-15.) Inoltre, dovrebbe essere eseguita una valutazione di conformità prima di poter essere immessi sul mercato dell'UE. (Articolo 19.) L'allegato III elenca i sistemi di IA nei seguenti settori come ad alto rischio:

- ✓ identificazione biometrica e categorizzazione delle persone fisiche
- ✓ gestione e funzionamento di infrastrutture critiche
- ✓ l'accesso all'istruzione e alla formazione professionale e la valutazione degli studenti a tali fini
- ✓ occupazione, gestione dei lavoratori e accesso al lavoro autonomo (assunzione, promozione, licenziamento)
- ✓ accesso e fruizione dei servizi privati essenziali e dei servizi e benefici pubblici
- ✓ forze dell'ordine (valutazioni individuali del rischio, poligrafi o strumenti simili, rilevamento di falsi profondi, valutazione dell'affidabilità delle prove, polizia predittiva, profilazione, analisi dei crimini riguardanti persone fisiche)
- ✓ gestione della migrazione, dell'asilo e del controllo delle frontiere
- ✓ amministrazione della giustizia e processi democratici.

La Commissione europea sarebbe autorizzata ad ampliare l'elenco se necessario, in base a una serie di criteri definiti. (Articolo 7). Fonte: https://www.loc.gov/item/global-legal-monitor/2021-05-26/european-union-commission-publishes-proposal-to-regulate-artificial-intelligence/.

[103] Come riportato in EUROPEAN DIGITAL RIGHTS (EDRi), *Civil society calls on the EU to put fundamental rights first in the AI Act*, November 30, 2021 in https://edri.org/our-work/civil-society-calls-on-the-eu-to-put-fundamental-rights-first-in-the-ai-act/.

Compreso l'obbligo obbligatorio per gli utenti dei sistemi di IA ad alto rischio di condurre e pubblicare una valutazione d'impatto sui diritti fondamentali, compreso l'impatto sulle persone, i diritti fondamentali, l'ambiente e l'interesse pubblico in generale.

- ✓ *Trasparenza pubblica coerente e significativa.*
  Compreso l'obbligo per gli utenti di registrare l'uso di sistemi ad alto rischio nella banca dati pubblica dell'articolo 60.
- ✓ *Diritti significativi e risarcimento per le persone colpite dai sistemi di intelligenza artificiale.*
  Come il diritto a non essere assoggettati a sistemi di IA in violazione del regolamento e delle pratiche vietate, il diritto a una spiegazione per le decisioni prese con l'ausilio dei sistemi di IA, e il diritto a un ricorso giurisdizionale.
- ✓ *Accessibilità durante tutto il ciclo di vita dell'IA.*
  Compresi i requisiti di accessibilità per tutti i sistemi di intelligenza artificiale.
- ✓ *Standard migliorati e a prova di futuro per i sistemi di intelligenza artificiale.*
  Limitare il processo di normalizzazione armonizzato ai soli aspetti genuinamente tecnici e garantire la partecipazione della società civile al processo.
- ✓ *Un'AIA davvero completo che funziona per tutti.*
  Garantire la privacy per le persone con disabilità; rimozione dell'ampia esenzione per i sistemi di intelligenza artificiale che fanno parte delle banche dati informatiche dell'UE su larga scala; e garantire un processo di applicazione solido e dotato di risorse che sia incentrato sui diritti fondamentali.

In definitiva, ove promuovessero la sorveglianza di massa e amplificassero disuguaglianze sociali e squilibri di potere, gli algoritmi alla base di decisioni pubbliche potrebbero mettere a rischio i diritti fondamentali, i processi e i valori democratici. Ecco perché la proposta di AIA delle istituzioni dell'Unione europea (UE) è un passo significativo a livello globale.

Ma, come ribadito sia da Unesco che da EDRi, l'AIA deve affrontare gli impatti strutturali, sociali, politici ed economici dell'uso dell'IA. Ciò garantirà che la legge sia 'a prova di futuro' e darà priorità alla protezione dei diritti fondamentali.

E soprattutto, per dirla con Peyron[104], *"questo dipende molto dal volto che si deciderà di dare all'IA, un volto che non può essere solo tecnico, ma che deve essere un volto umano, quello in cui solo siamo capaci di riconoscerci".*

[104] Cfr. LUCA PEYRON, *Intelligenza Artificiale: l'Italia lancia la strategia nazionale*, HuffPost 02/12/2021 in https://www.huffingtonpost.it/ entry/intelligenza-artificiale-litalia-lancia-la-strategia-nazionale_it_61a8d9b8e4b0451e55124 3df?utm_hp_ref=it-homepage, cit..

IL CASO WHATSAPP CONTRO L'AUTORITÀ DI VIGILANZA PER LA PROTEZIONE DEI DATI PERSONALI IN IRLANDA.

di Gaetano Guarino

SOMMARIO: 1. Introduzione; -2. Le norme rilevanti; - 3. L'intervento dell'autorità Irlandese; -4. Le obiezioni delle altre autorità; -5. L'intervento del comitato europeo per la protezione dei dati personali; -6. La difesa dell'azienda; -7. Rilievi critici.

This article is going to illustrate the caselaw Whatsapp/Data protection commission (the national autority of data protection law in Ireland). It begins illustrating the all european law from the General data protection regulation (GDPR) involved in this legal issue. Following this it is going to dimostrate the all infringments challenged, the binding action of European privacy autority and the verdict of DPC. It ends with some closing remarks.

1. Introduzione

L'oggetto di quest'articolo è il dispiegarsi della controversia tra Whatsapp e l'Autorità di vigilanza irlandese in materia di riservatezza, competente in quanto la sede legale della multinazionale in Europea è situata in questo stato membro. Tale disputa ha visto la partecipazione in modo significativo anche del Comitato europeo per la protezione dei dati personali, massima autorità europea in materia, e di altre autorità di vigilanza. Si tratta di una decisione particolarmente rilevante, dato che quest'applicazione di messaggistica gratuita viene utilizzata quotidianamente da milioni di utilizzatori in tutto il mondo e perché tale pronuncia potrà essere utilizzata in futuro per valutare anche la conformità di altre aziende del settore alla normativa europea.

2. Le norme rilevanti

Per meglio comprendere questa disputa ed i suoi esiti è opportuno cominciare dalla disamina normativa delle disposizioni rilevanti nel caso di specie.

Secondo il Regolamento europeo per la protezione dei dati personali (Reg. Ue 769/2016), ogni soggetto titolare del trattamento dei dati personali[105] deve fornire tutta una serie di informazioni al soggetto a cui richiede il rilascio dei suoi dati[106], se gli stessi non siano stati ottenuti presso l'interessato, quali: l'identità ed i contatti del titolare del trattamento e/o del suo rappresentante, nonché quelli del responsabile del trattamento dei dati personali; la finalità del trattamento; la base giuridica ed i relativi destinatari; la volontà o meno di trasferire i dati[107] ; la durata della loro conservazione[108].

Anche i diritti dell'interessato devono essere indicati: l'accesso, la rettifica, la cancellazione, la limitazione, l'opposizione e la portabilità, nonché la possibilità di revocare il consenso ed il diritto di reclamo. Infine, dovrà essere comunicato se sarà svolto su quei dati un processo automatizzato, come la profilazione, la sua logica e le sue conseguenze, la fonte dei dati e se essa è accessibile al pubblico[109].

Il regolamento precisa anche quando queste informazioni devono essere fornite: se si tratta di dati destinati alla comunicazione con l'interessato, al momento della prima comunicazione. E' ragionevole ipotizzare che queste informazioni debbano essere fornite durante la formazione del contratto online, tramite la visualizzazione di un'apposita schermata nel momento in cui il venditore è certo che il compratore effettui il suo acquisto. Si tratta dell'informativa privacy presente in molti contratti, di cui spesso viene chiesto il consenso o un cenno di presa visione tramite un click su un'apposita casella[110].

La normativa[111] stabilisce anche le modalità di fornitura di queste informazioni: in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro.

---

[105] Ex. Art. 4 n. 7 Reg. (UE) 2016/679: 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

[106] Ex: Art. 14 Reg. (UE) 2016/679 ibidem.

[107] Il trasferimento dei dati personali è disciplinato dagli art.44-45 e 46 del Reg. cit. ed è sottoposto ad uno stringente regime di garanzie.

[108] Cit. G. GUARINO, *Gli obblighi privacy nei contratti online, in Data Protection Law n. 2/2020.*

[109] G. GUARINO, *Gli obblighi privacy nei contratti online*, op. cit.

[110] G. GUARINO, *Gli obblighi privacy nei contratti online*, op. cit.

[111] Ex art.12 Reg. (UE) 2016/679 ibidem. G. GUARINO, *Gli obblighi privacy nei contratti online*, op. cit.

Se i dati sono stati forniti presso l'interessato[112] oltre a queste informazioni deve essere comunicato: se il trattamento dei dati è finalizzato a soddisfare un legittimo interesse del titolare o dei terzi e quale sia tale interesse, salvo che non siano prevalenti i diritti dell'interessato stesso.

Inoltre, va dichiarato se la comunicazione di dati è un obbligo legale o contrattuale, oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire questi dati, nonché le possibili conseguenze della loro mancata comunicazione.

Infine, bisogna render noto anche se il titolare del trattamento intenda trattare ulteriormente i dati per una finalità diversa da quella per cui essi sono stati raccolti e prima di tale ulteriore trattamento deve fornire all'interessato informazioni in merito a tale diversa finalità e ai suoi diritti.

L'articolo 5 del Regolamento individua i principi applicabili al trattamento di dati personali.

Anzitutto i dati devono essere trattati in maniera lecita, corretta e trasparente[113] e solo per fini determinati, espliciti e legittimi, nonché con modalità conformi a tali principi[114].

Per di più i dati possono essere utilizzati solo se adeguati, pertinenti e funzionali alla loro finalità[115].

Ancora, devono essere precisi, esatti secondo la terminologia del codice, e di conseguenza devono essere modificati, o cancellati se non rispettano tali caratteristiche[116].

In aggiunta devono essere conservati sempre per realizzare la finalità per la quale sono stati raccolti[117] e gestiti in modo da garantirne la sicurezza nel rispetto delle misure tecniche per la loro protezione[118].

A conclusione, come principio finale, viene sancita la responsabilità del titolare per il rispetto dei principi del trattamento[119].

---

[112] Ex art.13 Reg. (UE) 2016/679 ibidem
[113] principi di liceità, correttezza e trasparenza.
[114] principio di limitazione della finalità.
[115] principio di minimizzazione dei dati.
[116] principio di esattezza.
[117] principio di limitazione della conservazione.
[118] principio di integrità e riservatezza.
[119] principio di responsabilizzazione o accountability.

L'art. 60 del Reg. prevede che le autorità di vigilanza per la privacy a livello nazionale collaborino e cooperino tra loro e con quella europea, al fine di raggiungere un consenso qualora vi sia una problematica che riguardi più autorità. Tale cooperazione può estendersi anche ad attività ispettiva e di controllo. Alla capofila è riconosciuto un ruolo preminente essendo tenuta a comunicare alle altre il progetto di decisione e a tenere in considerazione le loro osservazioni, tant'è vero che la stessa è tenuta ad attivarsi non solo per rispondere a quest'ultime, ma anche affinché si raggiunga il consenso tra tutte le autorità.

L'art. 65 disciplina proprio l'ipotesi in cui debba intervenire con una decisione vincolante il comitato europeo per la protezione dei dati personali per garantire l'applicazione corretta e coerente del Regolamento europeo ai singoli casi. Quanto detto avviene, come è avvenuto nel caso di specie, laddove un'autorità abbia sollevato un'obiezione ad un progetto di decisioni di una capofila e quest'ultima l'abbia rigettata, non raggiungendosi in tal modo un consenso alla decisione da parte di tutte le autorità.

Completa il quadro delle disposizioni l'Articolo 83 del Regolamento che prevede le condizioni per infliggere le sanzioni amministrative, le quali devono essere effettive, proporzionate e dissuasive[120] e vanno commisurate in base a tutta una serie di indici:

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- la presenza di dolo o colpa;
- le misure attuate per attenuare il danno;
- il grado di responsabilità di titolare e responsabile tenuto conto delle misure di sicurezza;
- gli eventuali precedenti di titolare e responsabile;
- la cooperazione con le autorità di controllo;
- le categorie dei dati interessati;
- il modo in cui l'autorità è venuta a conoscenza della violazione;
- il rispetto degli eventuali provvedimenti precedentemente posti in essere dall'autorità;

[120] Le stesse si aggiungono alle misure di carattere preventivo quali gli avvertimenti al titolare o al responsabile sul fatto che i suoi trattamenti potrebbero violare il regolamento, la revoca delle certificazioni previsti dal regolamento a tutela della riservatezza ci si fa riferimento in particolare a quelle relative alle misure di sicurezza, e l'ordine di sospensione del trasferimento dei dati verso un paese terzo o un'organizzazione internazionale.

- l'adesione a codici di condotta o a meccanismi di certificazione;
- eventuali altri elementi aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Rilievo particolare assume il paragrafo 3 della medesima disposizione che recita: *"Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave".* Si tratta della disciplina del concorso di violazioni in materia di riservatezza.

Infine, vengono specificati i due fattori alla base dell'importo della sanzione e viene formulata una distinzione tra un gruppo di violazioni con una pena base e l'altro con pena aggravata.

Nel caso in cui si violino gli obblighi del titolare del trattamento e/o del responsabile del trattamento[121], quelli dell'organismo di certificazione[122] e/o quelli dell'organismo di controllo[123] l'importo della sanzione amministrativa pecuniaria è fino ad €10 000 000, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Le sanzioni sono raddoppiate se sono stati violati i principi del trattamento, comprese le norme in materia di consenso[124]; i diritti degli interessati[125]; le norme in materia di trasferimento[126]; altri obblighi stabiliti ex lege dagli stati membri, la non osservanza di un ordine, di una limitazione del trattamento o di un ordine sospensione dei dati o il negato accesso[127] e per l'inosservanza di tutti gli altri ordini e provvedimenti dell'autorità di vigilanza.

3. L'intervento dell'Autorità irlandese.

L'inchiesta dell'Autorità irlandese era partita nel 2018 e si è conclusa con la constatazione di alcune rilevanti violazioni della normativa, in particolare per quanto concerne le informazioni da fornire necessariamente agli utenti.

[121] Ex. artt. 8, 11, da 25 a 39, 42 e 43 GDPR.
[122] Ex artt. 42 e 43 GDPR.
[123] Ex art. 41, paragrafo 4 GDPR.
[124] Ex art. 5,6,7, e 9 GDPR.
[125] Ex artt. dal 12 al 22 GDPR.
[126] Ex artt. dal 44 al 49 GDPR.
[127] Ex art. 58 GDPR.

In dettaglio l'azienda non ha organizzato le informazioni in formato facilmente accessibile, ponendosi in contrasto con l'art. 12 del Regolamento UE; non ha fornito le informazioni obbligatorie ex art. 13 nonché quelle che dovevano essere fornite ai nuovi utenti nel momento in cui mostrava loro quali dei propri contatti erano anche utilizzatori della medesima app ex. art. 14; infine è stata accusata di aver violato il principio di trasparenza ex art. 5.
Per questi motivi l'autority richiedeva all'app di fornire tutte le informazioni richieste entro 3 mesi dalla data della decisione, nell'agosto 2020, ed emetteva un formale richiamo.

4. Le obiezioni delle altre Autorità.

Durante la procedura altre otto Autorità di vigilanza hanno aperto altrettanti procedimenti avendo l'Autorità condiviso con loro le informazioni raccolte.
Dette Autorità hanno formulato le seguenti osservazioni:

- l'Autorità irlandese non avrebbe analizzato adeguatamente il perché e come i dati dei soggetti interessati sarebbero stati processati, confondendo questi due punti;
- l'Autorità irlandese non avrebbe adeguatamente considerato le motivazioni addotte da Whatsapp nell'informativa sul perché i dati siano processati sia chiara e trasparente abbastanza per essere compresa dai soggetti interessati, poiché vi sono diverse ragioni per trattare i dati e vengono fatti soli vaghi riferimenti ai legittimi interessi, o interessi dell'impresa, o di altre aziende;
- l'Autorità irlandese non avrebbe fornito prove sul se il numero di telefono dei non utenti venga sottoposto o meno al processo di lossy-hashing e se i dati eventualmente coinvolti con questo procedimento siano da classificarsi come dati personali o non siano da considerarsi tali in ragione del tatto che tale procedimento non ricollegherebbe il dato all'individuo.

Ci sono state, inoltre, critiche su ulteriori aspetti, quali:

- il limitato scopo dell'inchiesta della capofila, nello specifico non sarebbe chiaro quali dati sono trattati e a quali dati di Whatsapp Facebook ha accesso;

- l'indulgenza dell'Autorità irlandese che si manifesta, in particolare, nella concessione di un periodo di 6 mesi all'App per adeguarsi e nell'ammontare della multa;
- Infine, riguardo all'interpretazione dell'art. 83 nel caso in cui ci siano più violazioni, si è criticato il fatto che per calcolarne l'ammontare ci si è basati sulla sanzione più severa. Il suo ammontare è apparso **"***hardly noticeable"* difficilmente visibile e non soddisferebbe i tipici caratteri delle sanzioni ex art 83: sanzioni effettive, dissuasive e proporzionate.

5. L'intervento del Comitato europeo per la protezione dei dati personali.

Tuttavia, dato che non vi è stato un consenso tra questi vari enti è scattata la procedura che prevede l'intervento a carattere vincolante del Comitato europeo ex art. 65, che si è conclusa con la decisione vincolante del Comitato del 28 luglio 2021. Nello specifico, l'Autorità europea ha fornito diversi criteri alla capofila non solo per gestire le problematiche nel merito, ma anche per risolvere le criticità relative all'eccessiva durata del procedimento e all'ammontare di sanzioni effettive.
Riguardo la modalità con la quale comunicare le informazioni obbligatorie, il Comitato ha stabilito che devono essere dettagliate, molto più di quanto l'App le abbia formulate in passato, facilmente accessibili, senza l'uso di una pluralità di collegamenti a documenti che possono essere difficili da trovare e da comprendere.
In particolare, si è evidenziata la necessità di fornire informazioni in modo ordinato, non sparso e frammentario, al fine di evitare di dover richiedere all'utente lo sforzo di ricercarle in diversi luoghi informatici. Anche se non vengono vietati i link a pagine contenenti le informazioni, riconoscendo che possono esserci delle buone ragioni che ne giustificano l'utilizzo, i titolari del trattamento devono assicurare che il soggetto interessato possa vedere tutte le informazioni rilevanti in modo semplice, evitando così incongruenze.
Per di più si è prescritto che l'App non deve fornire contestualmente l'informativa privacy e i termini legali di utilizzo, perché l'elevata mole di informazioni potrebbe scoraggiarne la lettura.
Però si è riconosciuto che l'azienda ha comunque fatto dei passi avanti durante l'istruttoria tra cui evitare il continuo scorrimento delle informazioni, eliminando modalità

scorciatoia che davano la possibilità agli utenti di evitare di vedere e di leggere le informazioni dopo l'home page.

Circa il contenuto delle informazioni da fornire ex art. 13 comma 1 e 2, l'Autorità ha agito ad ampio spettro chiarendo obbligo per obbligo sia le violazioni riscontrate sia come si sarebbe dovuta comportare l'azienda. Per questo motivo tale decisione può considerarsi rilevante anche in futuro per aziende che svolgono servizi simili.

A sua difesa l'App ha sostenuto che i dettagli contenuti nell'informativa privacy erano soddisfacenti, essendo, tra l'altro, in linea con quelli forniti dalle altre aziende del settore. L'Autorità ha rigettato tale tesi sostenendo che un settore industriale non può stabilire il livello di dettagli sufficienti e sottolineando che nel caso di specie si era rilevata una grande quantità di testo che in realtà comunicava molto poco.

Per quel che concerne l'art. 13, ovvero le finalità del trattamento e la sua base giuridica, il Comitato ha prescritto che tali elementi devono essere dichiarati facendo riferimento alla precisa categoria dei dati a cui appartengono e alle specifiche operazioni di trattamento a cui verranno sottoposti.

Il tutto affinché la persona interessata possa essere messa nelle condizioni di poter identificare e conoscere la base giuridica di ogni trattamento e la relativa norma europea o nazionale che ne sancisce l'obbligatorietà; se vi possono essere più basi giuridiche per un trattamento l'informativa deve essere sufficientemente dettagliata per consentire di comprendere quando l'ente agisce in base ad una norma e quando in base ad un'altra.

Riguardo i destinatari dei dati personali o le categorie di destinatari, se è specificata una categoria, o un destinatario questo dato, quest'identificazione deve essere la più specifica possibile, e le informazioni dovrebbero essere relative ai servizi ricevuti dagli utenti e alle categorie di dati rivelati ai destinatari. I soggetti interessati dovrebbero poter identificare quali categorie di dati sono trasferiti, a chi sono destinati e perché.

Sul trasferimento di dati è stato affermato che l'informativa deve fornire anche i dettagli sull'esistenza di una decisione di adeguatezza della Commissione europea in materia di trasferimento, e non solo un link riguardo tutte le decisioni in generale, nonché vanno dichiarate dettagliatamente le clausole contrattuali alla base del trasferimento.

Particolare attenzione è, poi, riservata al periodo di durata della conservazione dopo l'uso del servizio. L'azienda sosteneva che questo può dipendere dalla natura dei dati,

dalle norme o dal procedimento applicabile. L'Autorità ha stabilito che tale giustificazione è insufficiente e che devono essere fornite informazioni relative i criteri di conservazioni.

Tra le informazioni sui diritti dei soggetti interessati quelle sulla possibilità di ritirare il consenso devono essere incluse in un'apposita sezione sul consenso perché deve essere spiegato chiaramente che cancellare il consenso non ha effetti sul trattamento basato sul consenso precedentemente prestato. Bisogna spiegare che in tal caso l'utente non viola la legge e nemmeno l'App.

Per di più se la fornitura di informazioni è un requisito legale, o contrattuale, deve essere chiaro che devono essere richieste le minime informazioni necessarie e non informazioni più specifiche.

In materia di informazioni ai non utilizzatori la decisione sostiene che Whatsapp non soddisfa i requisiti dell'art. 14 sulla trasparenza, in relazione ai dati ottenuti da soggetti diversi rispetto alla persona interessata. Questo trattamento avviene quando un non utente si iscrive all'App che gli rivela gli altri suoi contatti telefonici che sono utenti e rileva a quest'ultimi che vi è un nuovo utente. Tuttavia, l'autorità ha accettato il fatto che l'App potrebbe non fornire informazioni non individuali ai non utenti anche se si è scoperto che la procedura non porta all'anonimizzazione dei dati personali raccolti.

Circa il procedimento denominato lossy hashing, il comitato ha stabilito che i numeri di telefono che sono sottoposti a questo processo sono dati personali, perché possono essere collegati ad un piccolo gruppo di individui e attraverso le informazioni sul genere si potrebbe stringere ancor di più l'identificazione.

Veniva, inoltre, rigettata la critica relativa allo scopo dell'inchiesta dichiarando che non via erano prove che espandendola ci sarebbero state conclusioni differenti.

Rispetto alle sanzioni l'Autorità ha imposto all'azienda di cambiare l'informativa privacy entro 3 mesi, anche se la stessa ha tentato di difendersi sul punto sostenendo la gravosità di tale impegno. In tal caso l'Autorità ha replicato sottolineando che l'azienda ha sufficienti mezzi per soddisfare l'obiettivo.

L'Autorità ha, poi, rigettato l'altra obiezione secondo cui l'Autorità dovrebbe mostrare indulgenza nel suo approccio in modo simile con quello mostrato con le aziende più piccole del settore di rilievo nazionale. Questo perché le grandi aziende di rilevo internazionale hanno più ingenti risorse che le consentono di soddisfare standard più elevati.

Sul quantum della sanzione l'Autorità europea si è basata sulla natura e sulla gravità delle violazioni, nonché sulla loro durata che è andata avanti almeno dal 25 maggio 2018. Infine, si è basata sull'alto numero di soggetti interessati potenzialmente colpiti. Allo stesso tempo i fattori attenuanti erano: la natura limitata dei dati trattati riguardo i non utenti e i cambiamenti già effettuati dall'App sull'informativa.
Nello specifico il comitato ha statuito che l'art. 83 co. 4 e 5 fornisce un tetto massimo, impostato in base ad un ammontare o al fatturato, precisando che quest'ultimo è considerato quello che colpisce meglio tutte le componenti di un gruppo di azienda. Pertanto, il fatturato deve essere valutato direttamente non solo per assicurare che la multa non violi il massimale, ma anche come punto di partenza per stabilire l'ammontare della sanzione.
Andando più nel dettaglio, il Comitato ha anche dichiarato che dato che l'ammontare totale della sanzione non deve eccede l'ammontare previsto per la più grave delle violazioni, la più grave deve essere considerata non quella per la quale è prevista una sanzione più elevata ma quella più significativa, più importante.
Di conseguenza l'interpretazione dell'art. 83 della capofila era scorretta ed avrebbe comportato che non sarebbe rilevato se un titolare avesse commesso una o più infrazione, perché solo la più grave sarebbe stata considerata. Perciò la sanzione proposta falliva nel riflettere in modo adeguato le serietà e la severità delle violazioni o nell'avere effetti dissuasivi sull'App, come recita letteralmente il testo: "adequately reflect the seriousness and severity of the infringements" or have "a dissuasive effect" on WhatsApp.
Quanto al termine di 6 mesi inizialmente concesso dall'autorità capofila è stato considerato eccessivamente clemente, perché se fosse stato confermato avrebbe messo pressione alle altre autorità, che avrebbero dovuto concedere termini ancora più generosi alle aziende più piccole, dunque, detto termine è stato considerato non appropriato e proporzionato, e pertanto è stato ridotto a 3 mesi.
Per tutte queste ragioni il Comitato europeo per la protezione dei dati personali ha aumentato penalità inflitta dall'autorità garante irlandese fino a 250 milioni di euro con una decisione vincolante pubblicata il 2 settembre 2021.

6. La difesa dell'azienda.

Whatsapp si è difesa dichiarando che la sanzione comminata fosse sproporzionata, dato che all'inizio del procedimento essa era pari a soli 50 milioni di euro.

Nello specifico la sua tesi difensiva si basava su 5 punti:
1 la capofila avrebbe dato una nuova e soggettiva interpretazione delle norme in materia di trasparenza e/o in alternativa con più alti standard di conformità di cui l'app non avrebbe ricevuto in anticipo notizia;
2 avrebbe adottato un approccio binario sulla conformità, non considerando che alcune, ma non tutte, le informazioni richieste sono state fornite agli utenti;
3 non si sarebbero considerati i suoi sforzi e la sua buona fede per mettersi in regola;
4 non si sarebbe considerato il suo è impegno con la Commissione per un'azione conforme alle norme europee.
L'Autorità irlandese, dinanzi al quale il procedimento è proseguito dopo la decisione europea, ha dichiarato riguardo al punto 2 (la parziale fornitura di informazioni) che può essere preso in considerazione per determinare la sanzione.
Riguardo al punto 1 ha dichiarato che non solo non è stato provato cosa i titolari dei trattamenti delle aziende del settore devono fare, ma che non sono i soggetti competenti a stabilire gli obblighi in tema di trasparenza.
Inoltre, è stato considerato non appropriato coinvolgere la commissione in questioni riguardanti il rispetto del GDPR.
Infine, gli sforzi, sebbene fossero stati apprezzati, sono stati considerati molto limitati.
Whatsapp ha impugnato la decisione definitiva della capofila, che ha confermato quanto stabilito dal Comitato, dinanzi all'alta Corte irlandese che ha dichiarato l'impugnazione ammissibile previa la costituzione in giudizio dell'Autorità di vigilanza irlandese, di quella europea e dell'Avvocato generale.
L'azienda cerca con questa azione di annullare la decisone dell'autorità irlandese e di provare che alcune norme del national privacy act irlandese del 2018[128] (la legge in base alla quale ha agito l'autorità dello stato membro) sono invalide e incostituzionali nonché non rispettose della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), perché emetterebbero delle sanzioni penali. La corte si è riservata, prendendo del tempo per decidere.

[128] In particolare, la sezione 110 del the Irish Data Protection Act del 2018.

7. Rilievi critici.

La sanzione all'azienda di messaggistica istantanea Whatsapp, è stata dovuta dal mancato rispetto delle norme che prevedono la necessaria comunicazione agli utenti di una serie di informazioni con modalità che ne assicurino leggibilità e conoscibilità, nonché dalla poca trasparenza dimostrata sia a livello generale, sia quando un nuovo utente effettua l'iscrizione all'App.

Si osserva che il perno di tutta l'informativa sulla riservatezza è la finalità, ovvero il motivo per il quale le informazioni sono richieste, di modo da rendere l'utente consapevole del perchè le informazioni da lui fornite saranno trattate, al fine di permettergli una scelta consapevole.

Altro elemento fondamentale è la base giuridica: la citazione delle disposizioni di legge che consentono la richiesta di queste informazioni.

Dall'analisi della decisione si può dedurre che ben poca enfasi è stata lasciata a questi due elementi, anche se essi sono alla base di tutti i trattamenti utilizzati e ne sono al contempo il limite, in virtù del principio di minimizzazione. Sarebbe stato opportuno stabilire che entrambi dovevano avere un ruolo centrale e preminente nell'informativa, per rispondere alla domanda dell'utente del perché era necessario fornire dei dati e quale operazione quest'azienda effettuava.

In parte quest'elemento è ripreso nella decisione, specialmente nella parte sul trasferimento dei dati, ma sembra che sia accantonata rispetto alla altre.

Altro problema di rilievo è l'adattamento alla pratica, alla prassi di tale decisione che reca con sé il rischio di un'eccessiva burocratizzazione a ritmo di consensi e fornitura delle informazioni, che rischia di vanificare la tutela della riservatezza, in quanto diritto fondamentale dell'utente.

Lo scopo della regolamentazione non è quello di consentire alle aziende di utilizzare i dati personali, rispettando delle formalità, ma di tutelare la riservatezza degli utenti di fronte a pratiche, aziende ed anche veri e propri contratti che milioni di persone, più o meno consapevolmente, stipulano online ogni giorno. Spesso il consenso e la fornitura di informazioni sono subordinati all'accesso ad un servizio che l'utente considera un bisogno impellente, necessario e quindi non presta la necessaria attenzione. Pertanto, bisognerebbe sensibilizzare sia le aziende, sia gli utenti ad un corretto uso dei dati personali.

Questo non toglie che il comportamento dell'azienda di messaggistica viola a tutti gli effetti la normativa, secondo le autorità competenti, e quindi sembra necessaria una riflessione sull'ammontare della conseguente sanzione e sul suo effetto dissuasivo.

I fenomeni societari in generale e su larga scala hanno come effetto quello di mascherare, di celare e di rendere più difficile capire l'organigramma aziendale, quali sono i soggetti che vi lavorano, quelli che prendono le decisioni, quelli che le eseguono, gli eventuali controllori interni e responsabili esterni. Vi è sempre un rischio di un rimpallo di responsabilità, o comunque forti difficoltà a trovare uno, o più colpevoli, di qualunque violazione delle norme.

Al contempo la persona giuridica, oltre ad avere una sede legale deve avere anche delle coordinate bancarie per ricevere gli introiti delle sue attività, una specie di indirizzo per i suoi debitori dove effettuare le loro prestazioni.

Di conseguenza una sanzione pecuniaria evita il rischio del rimpallo di responsabilità, ed assicura una più celere ed efficace esecuzione. La forza dissuasiva della sanzione si rinviene proprio nell'elevato ammontare, perché altrimenti rischia di essere vista solo come una delle tante voci di costo aziendali e non essere percepita come una sorta di punizione per aver violato la legge. D'altronde queste violazioni, in generale ed anche in questo caso sono compiute nell'ottica di ridurre i costi e massimizzare profitti, che, come la storia dimostra, porta sempre con sé rischi elevati e interrogativi etici e morali non di poco conto.

La difesa dell'azienda dubita se tale sanzione sia da qualificare come penale o meno. L'interessante interrogativo, che reca con sé la necessaria applicabilità di tutta una serie di garanzie a favore del reo, si pensi alla conoscibilità della norma penale e all'irretroattività della stessa che tanto fanno discutere in sede anche europea, non sembra apparentemente avere grandi effetti.

Questo perché l'ammontare di queste violazioni è proporzionato anche alla gravità delle violazioni ed al numero dei soggetti coinvolti; perciò, un'azienda che tratta milioni di utenti e milioni di dati, non può non aspettarsi sanzioni molto elevate, considerando anche che si tratta di un rimprovero che si basa sulla responsabilità non dell'uomo medio, ma del professionista, dell'azienda di settore che ha il dovere ed il potere di adeguarsi alle norme, ben sapendo che rischia sanzioni.

Sarà la corte EDU a sciogliere questo nodo, se lo riterrà ammissibile.

Note bibliografiche:

CONOR HUMPHRIES, "WhatsApp fined a record 225 mln euro by Ireland over privacy", 2 settembre 2021, link: https://www.reuters.com/technology/irish-data-privacy-watchdog-fines-whatsapp-225-mln-euros-2021-09-02/

RUTH BOARDMAN, "Irish DPC WhatsApp decision: What do you need to know?", 28 settembre 2021, link: https://iapp.org/news/a/irish-dpc-whatsapp-decision-what-do-you-need-to-know/

AODHAN O'FAOLAIN, "WhatsApp Ireland given permission to challenge DPC's €225m fine", 8 novembre 2021, link: https://www.irishtimes.com/business/technology/whatsapp-ireland-given-permission-to-challenge-dpc-s-225m-fine-1.4722727

"L'EDPB chiede all'autorità di controllo irlandese di modificare la decisione WhatsApp e fornisce chiarimenti sulla trasparenza e sul calcolo dell'importo della sanzione pecuniaria dovuta in presenza di violazioni multiple", 2 settembre 2021, link: https://edpb.europa.eu/news/news/2021/edpb-requests-irish-sa-amends-whatsapp-decision-clarifications-transparency-and_it

RUTH BOARDMAN, "Irish Data Protection Commission WhatsApp decision: what do you need to know?", ottobre 2021, link: https://www.twobirds.com/en/news/articles/2021/uk/irish-data-protection-commission-whatsapp-decision

LA CYBERSECURITY TRA PRIVACY E INNOVAZIONE DIGITALE

Francesco Lo Chiatto

SOMMARIO: 1. Introduzione -2. Cybersecurity e disciplina giuridica -3. Cyberminacce e linee guida per la protezione -4. Casi recenti di attacchi informatici e il Polo Strategico Nazionale -5. Sicurezza e insicurezza digitale, verso una nuova alfabetizzazione.

This work, preceded by an introduction, addresses the legal discipline of cybersecurity, first giving a definition of it, and then addressing all its dynamics, both legal and applicative. The European Directive 2016/1148 transposed in Italy with Legislative Decree n.65/2018, addresses the issue of cybersecurity, defining the necessary measures aimed at achieving a high level of security of information systems. On 7 June 2019, the Cybersecurity Act, Regulation on Cybersecurity, was published, which completes the previous legislative developments. The objective of the same is to create a single regulatory framework in order to harmonize the regulation of cyber attacks throughout the European territory and in order the increase the security of IT products and services and increase consumer confidence. A brief mentionis made of what are the cyber threats and the recent attacks on public instititutions. The work ends with the hope for Italy to be able to make that digital transition, through an ever increasing digital literacy.

1. Introduzione

Il presente lavoro analizza la disciplina giuridica della cybersecurity, fornendo dapprima una definizione della stessa, e successivamente affrontando tutte le sue dinamiche, sia giuridiche che applicative. Con la Direttiva Europea 2016/1148, recepita in Italia con Decreto Legislativo n. 65/2018, si è trattato il tema della cybersecurity, definendo le misure necessarie volte a conseguire un elevato livello di sicurezza dei sistemi informativi. Successivamente, il 7 giugno 2019 è stato pubblicato il Cybersecurity Act, Regolamento sulla Cybersicurezza, che è andato a completare i precedenti sviluppi legislativi. Obiettivo dello stesso è creare un quadro normativo unico al fine

di armonizzare la regolamentazione relativa agli attacchi cibernetici su tutto il territorio europeo, aumentare la sicurezza dei prodotti e dei servizi informatici e far accrescere la fiducia dei consumatori. Nel corso del presente lavoro viene poi fatto un breve cenno a quelle che sono le minacce informatiche e ai recenti attacchi ad istituzioni pubbliche, concludendo con l'auspicio per l'Italia di poter compiere quella transizione digitale, attraverso un'alfabetizzazione digitale sempre più crescente.

2. Cybersecurity e disciplina giuridica.

Quando parliamo di cybersecurity, il primo passo da compiere è quello di comprendere nei minimi dettagli il significato della parola che nella sua traduzione letterale dall'inglese vuol dire "sicurezza cibernetica". Il termine ha, però, un'ulteriore traduzione, dal greco, kybernetes, che vuol dire "controllo". Tuttavia, tra le diverse definizioni che possono essere attribuite alla parola cybersecurity, quella più frequentemente utilizzata è quella di cui alla norma ISO/IEC 27000:2014 secondo cui per cybersecurity si intende quella pratica che consente ad una organizzazione, a un cittadino, a una nazione di proteggere i propri asset fisici e la confidenzialità. Dunque, per cybersecurity si intende la protezione dei dati e delle informazioni tra un mittente e uno o più destinatari nei confronti di terze parti e la integrità e la disponibilità delle proprie informazioni dalle minacce che arrivano dal cyberspazio. Tale protezione può avvenire attraverso misure di carattere tecnico e organizzativo che possono garantire la riservatezza delle informazioni, l'integrità dei dati e la disponibilità degli stessi. Il termine cybersecurity, quindi, fa riferimento alla sicurezza informatica che consiste nel difendere i computer, i server, i dispositivi mobili, e le reti dagli attacchi dannosi. La cybersecurity può essere utilizzata per rendere più sicura una rete, per rendere più sicure delle applicazioni, per la sicurezza delle informazioni, per prevedere delle procedure da utilizzare nel caso di disaster recovery e per la formazione degli utenti finali[129]. La sicurezza informatica, quindi, va a coinvolgere molteplici ambiti, riguardanti la vita privata, la vita pubblica, e quella aziendale, dove la protezione delle informazioni risulta di vitale importanza. E' fondamentale, a tale proposito, predisporre delle misure volte a tale tutela, seguendo delle linee guida che possano aiutare nella prevenzione di rischi, tali da portare una perdita, in seguito a un evento inatteso, o a

[129] Cfr. "Cos'è la Cybersecurity?", link: https://www.kaspersky.it/resource-center/definitions/what-is-cyber-security

uno scostamento da quelli che sono i risultati previsti. In tal senso risulta necessario richiamare la norma ISO 27001 che volge la sua attenzione alla standardizzazione delle modalità atte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. E' necessaria, quindi, una particolare pianificazione della sicurezza, nonché la valutazione e la gestione del rischio. Il legislatore europeo non è rimasto inerte dinanzi a tali problematiche ed è intervenuto con la Direttiva Europea 2016/1148, recepita in Italia con Decreto Legislativo n. 65 del 2018, affrontando il tema della cybersecurity, definendo quelle che sono le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi e prevedendo, tra l'altro, la notifica degli incidenti di sicurezza informatica subiti[130]. Il decreto 65/2018 ha individuato i soggetti competenti a dare una preliminare attuazione alla cyber difesa europea, quali Ose e Fsd[131]. Gli Ose sono le organizzazioni pubbliche o private che forniscono servizi essenziali per la società e l'economia nei settori bancario, dell'energia, dei trasporti, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile, delle infrastrutture digitali e del campo sanitario. Gli Fsd, invece, sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con almeno 50 dipendenti e con bilancio annuo non inferiore ai 10 milioni di euro. Tali soggetti devono adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi, prevenire e minimizzare l'impatto degli incidenti di sicurezza delle reti e dei sistemi informativi e sono tenuti a notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante sulla continuità e sulla fornitura del servizio, informando anche l'Autorità nazionale competente Nis. Gli Ose e i Fsd devono comunicare al CSIRT, Computer Security Incident Response Team, la notifica di detti incidenti informatici. Più recentemente il 7 giugno 2019 è stato pubblicato il Regolamento Ue 2019/881 denominato "Cybersecurity Act", Regolamento sulla cybersicurezza. Tale Regolamento[132] va a completare le precedenti azioni della Ue, come la direttiva Nis 2016/1148 e il Gdpr 2016/679. Il Cybersecurity Act introduce un complessivo quadro normativo volto ad armonizzare la regolamentazione degli attacchi

130 La Direttiva è consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=ES
131 Il Decreto è consultabile al seguente link: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg
132 Il Regolamento è consultabile al seguente link: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

cibernetici su tutto il territorio europeo. Questo passaggio risulta fondamentale, in quanto la società sta attraversando una trasformazione digitale e con l'avvento dell'Internet of Things (IoT) maggiori sono i rischi connessi alla sicurezza informatica essendo maggiore la vulnerabilità agli attacchi e ai pericoli connessi. Gli obiettivi del Cybersecurity Act sono quelli di creare un mercato unico della sicurezza cibernetica, in termini di prodotti, servizi e processi, così da far accrescere la fiducia dei consumatori nelle tecnologie digitali. Tale Regolamento si compone essenzialmente di due parti: la prima in cui vengono specificati ruolo e mandato dell'agenzia europea sulla sicurezza cibernetica, ENISA; la seconda in cui si istituisce un sistema europeo per la certificazione della sicurezza informatica di dispositivi, prodotti e servizi digitali. L'ENISA è l'agenzia europea per la sicurezza delle reti e dell'informazione, istituita nel 2004 con mandato limitato sia sotto il profilo della competenza sia dal punto di vista temporale. L'agenzia con il Cybersecurity Act è stata trasformata in un organo permanente, il cui compito è gestire gli incidenti insieme agli Stati membri, oltre occuparsi dello sviluppo e dell'attuazione delle politiche comunitarie e della predisposizione di schemi europei per la certificazione sulla sicurezza cibernetica. Il quadro normativo sulle certificazioni riguardanti la sicurezza in internet, non solo favorisce un approccio comune, ma migliora la protezione cibernetica dei prodotti digitali, creando così una maggiore fiducia nei consumatori. Il Cybersecurity Act, quindi, non crea schemi di certificazione direttamente operativi, ma definisce un quadro regolatorio per la loro creazione, venendo gli stessi, come detto, realizzati da Enisa e approvati dalla Commissione con atti di esecuzione, riconosciuti in tutti gli Stati membri. Obiettivo degli schemi di certificazione è far si che i servizi, i sistemi, i processi adottati, utilizzati, mirino alla protezione dei dati che vengono trattati e che vi sia una corretta divulgazione degli stessi al fine di prevenire incidenti di vario genere. Questi processi devono prevedere criteri di security by design, per la progettazione di prodotti e servizi, e criteri di security by default. Il Cybersecurity Act prevede infatti tre livelli di certificazione differenti ai sensi dell'art. 52 commi 5,6 e 7[133], quali: un livello di affidabilità base per il quale il produttore, fornitore, può ricorrere all'autocertificazione se questa viene prevista; un livello di affidabilità sostanziale, per il quale la valutazione di sicurezza è effettuata al fine di ridurre al minimo i rischi come incidenti e attacchi informatici, cui seguirà un riesame per verificare l' assenza di invulnerabilità

[133] Consultabile al seguente link: https://lexparency.org/eu/32019R0881/ART_52/

e un test che dimostri che i prodotti e i servizi adempiano a quegli obblighi di sicurezza; per finire, un livello di affidabilità elevato per il quale la valutazione di sicurezza è effettuata al fine di ridurre al minimo il rischio di attacchi informatici avanzati, commessi da soggetti, attori, hacker che dispongono di abilità e risorse molto importanti. Anche in quest'ultimo caso la valutazione che viene posta in essere comprende un test per dimostrare che i prodotti funzionino correttamente e assicurino un alto grado di sicurezza allo stato tecnologico più avanzato, e un penetration test che dimostri l'invulnerabilità dinanzi ad attacchi più avanzati. In tal senso anche il Nist, il National Institute of Standards and Technology, prevede dei macroprocessi, cioè delle linee guida tali da apportare a livello globale un corretto utilizzo e una sicurezza avanzata dei sistemi informatici come identificazione, protezione, rilevazione, ripristino. Una buona protezione dei sistemi informatici parte da una precedente analisi del rischio, la quale valuta le varie minacce in termini di probabilità, e, quindi, predispone le giuste contromisure. Gli eventi che possono mettere a rischio la sicurezza informatica possono derivare da eventi accidentali, come un uso difforme dei sistemi, dei guasti imprevisti, la mancata attuazione delle linee guida o eventi indesiderati derivanti da attacchi malevoli o da un accesso ai sistemi senza le dovute autorizzazioni. Questi attacchi malevoli vengono fatti tramite una rete internet, utilizzando software particolari al fine di poter penetrare nel sistema e accedere a tutti i dati presenti, con l'intento di carpirli o anche distruggerli a seconda delle finalità. Gli attacchi sono vari e possiamo distinguere alcuni come i buffer overflow, DoS, hacking, keylogging, backdoor, spyware. La protezione da questi attacchi informatici può avvenire con mezzi di sicurezza fisica, al fine di impedire l'ingresso fisico ai locali protetti, tenendo i server in luoghi sicuri. Ma tuttavia la vera sicurezza informatica è garantita da software che attraverso i firewall riescono a bloccare gli attacchi malevoli, cioè tutti quei tentativi di accesso senza le dovute autorizzazioni. Un altro strumento fondamentale per preservare i dati è il backup, che consente una copia di sicurezza dei dati, al fine di non perderli in caso di attacco hacker andato a buon fine. Nel caso un'hacker riesca a penetrare all'interno dei server, obbliga il titolare, ai sensi dell'art. 33 del Gdpr 679/2016, a comunicare la violazione all'autorità di controllo entro le 72 ore da cui viene a conoscenza del data breach[134]. L'autorità di controllo è competente per l'esercizio dei compiti e dei poteri assegnatale sul territorio del proprio stato membro, così

[134] Il testo dell'articolo è consultabile al seguente link: https://www.privacy-regulation.eu/it/33.htm

come previsto dall'art.55 del Gdpr 679/2016[135], e quindi se la violazione si verifica in un determinato Stato membro sarà l'autorità garante di quello Stato a cui dovrà essere notificata la violazione ai sensi dell'art. 33. Il legislatore europeo è intervenuto quindi al fine di rendere sempre più sicuro il trattamento dei dati, sia da parte di persone fisiche, sia da persone giuridiche, predisponendo regolamenti e linee guida, tali da porre una strada maestra da seguire e rispettare. In ultimo, le certificazioni previste dal Cybersecurity Act consentiranno agli utenti di conoscere il livello di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC nel mercato dell'Unione, garantendo un miglior funzionamento del mercato europeo, con un ottimo grado di protezione dei prodotti, già in maniera predefinita.

3. Le Cyberminacce e linee guida per la protezione

A livello globale le minacce informatiche continuano ad aumentare e solo nel 2019 vi sono stati il doppio degli attacchi informatici rispetto all'anno precedente. Tali attacchi informatici coinvolgono spesso strutture caratterizzate da una concentrazione di dati particolari, come ospedali, luoghi di cura, o enti pubblici. Questi continui attacchi determineranno un aumento della spesa pubblica per soluzioni di Cybersecurity che, entro il 2022, raggiungerà i 133, 7 miliardi di dollari. Tutti gli Stati stanno predisponendo investimenti al fine di poter ridurre tali rischi. Ad esempio: gli Stati Uniti hanno creato un framework di cybersecurity; il governo britannico ha pubblicato un documento "10 steps to cybersecurity"; l'Australia con l'Australian Cyber Security Centre pubblica costantemente indicazioni per contrastare le nuove minacce informatiche. Le minacce possono essere varie, come il Cybercrimine attraverso il quale singole persone o gruppi di persone attaccano i sistemi informatici di una determinata azienda, ente locale, ospedale, per ottenere un ritorno economico o provocare delle interruzioni che comportano perdita di soldi; i cyberattacchi, che, invece, hanno la finalità di raccogliere informazioni per lo più politiche; si pensi, infine, al cyberterrorismo che ha lo scopo di minare la sicurezza dei sistemi di sicurezza, al fine di terrorizzare le persone, rendendo gli obiettivi sensibili più vulnerabili. Queste intrusioni da parte di attori esterni in sistemi informatici avvengono attraverso i malware, software che vengono creati con l'obiettivo di provocare il malfunzionamento di computer, mediante allegati di e-mail o do-

[135] Il testo dell'articolo è consultabile al seguente link: https://www.privacy-regulation.eu/it/55.htm

wnload apparentemente legittimi. Diversi sono i malware, come il virus che è un programma capace di replicarsi autonomamente e che attaccandosi a un file pulito si diffonde nell'intero sistema informatico infettandone i file con il suo codice malevole; o il trojan che è un malware mascherato e che può causare danni e raccogliere i dati; o, ancora, lo spyware che è un programma che registra segretamente le azioni dell'utente per far si che i cybercriminali sfruttino le informazioni a proprio vantaggio. Altri esempi di malware sono il ransomware che blocca l'accesso ai file e dati dell'utente minacciando di cancellarli e ancora gli adware e i botnet. Le modalità con cui questi possono attaccare le reti private e quindi entrare in personal computer e avere accesso a informazioni e ai dati più disparati sono varie, come ad esempio il pishing, ovvero una tecnica con la quale vengono inviate e-mail che sembrano provenire da aziende legittime al fine di riuscire a carpire dati sensibili, quali dati di carte di credito o altre informazioni personali. Un altro esempio è l'attacco man-in-the-middle che è una minaccia informatica in cui un cybercriminale intercetta le comunicazioni fra due persone allo scopo di sottrarne i dati e questo può accadere quando la rete wifi non è protetta. L'attacco denial of service invece si ha quando i cybercriminali impediscono a un sistema informatico di poter essere utilizzato, sovraccaricando reti e server. Compito della cybersecurity è proprio quello di tutelare l'utente attraverso protocolli crittografici per crittografare messaggi, e-mail, file ed altri dati importanti. Il software di sicurezza svolge un ruolo fondamentale, in quanto durante la scansione del computer se ravvisa un codice malevolo lo mette in quarantena e poi lo rimuove. I protocolli di sicurezza elettronica più delle volte possono confinare i programmi potenzialmente dannosi in una bolla virtuale, separata dalla rete dell'utente, per analizzarne il comportamento e determinare la natura. Pertanto, l'utilizzo di un buon software, a volte, può non risultare sufficiente e quindi la prima azione a difesa del proprio computer è seguire delle indicazioni semplici ma fondamentali per far si che il rischio di attacchi indesiderati sia ridotto al minimo. Sarà necessario quindi aggiornare il software e il sistema operativo per avere patch di sicurezza sempre più recenti, utilizzare software antivirus e password complesse, non aprire allegati di e-mail di cui non si conosce il mittente, né cliccare su link contenuti nei messaggi e-mail e utilizzare reti Wi-fi non protette negli spazi pubblici che espongono l'utente ad attacchi Man-in-the-Middle[136]. In questo periodo di pandemia, con l'aumentare di professionisti che lavorano da casa,

[136] Cfr. "Cos'è la Cybersecurity?", link: https://www.kaspersky.it/resource-center/definitions/what-is-cyber-security

maggiori sono stati gli attacchi informatici e infatti l'Italia risulta essere il quarto paese al mondo più colpito da minacce informatiche correlate al Covid-19. Società di sicurezza informatica, contano sul nostro Paese circa 131.197 attacchi tra e-mail di spam, malware e siti maligni a tema pandemia[137]. Un gruppo chiamato Void Balaur, criminali informatici, dal 2015 ha compiuto circa 3.500 attacchi in tutto il mondo, colpendo società informatiche, società di telecomunicazioni, attivisti, giornalisti e leader religiosi. Il gruppo è dotato di tecniche molto avanzate, tali da poter carpire la posizione dei singoli cellulari, chi ha chiamato una persona, la durata, e la posizione da dove è avvenuta la chiamata. Questo gruppo, oltre a società di telecomunicazioni in Russia e negli Stati Uniti, ha nelle sue mire molti attivisti, difensori dei diritti umani, come successo in Uzbekistan o, nel 2020, con i candidati presidenziali in Bielorussia. Nel 2021 il gruppo ha preso di mira politici, funzionari governativi di Ucraina, Slovacchia, Russia, Kazakistan, Armenia, Norvegia, Francia, Italia. Void Balaur gestisce anche molti siti di pishing attraverso i quali vengono mossi molti attacchi ad aziende private su commissione di clienti disposti a pagare pur di carpire dati e segreti aziendali[138].

4. Casi recenti di attacchi informatici e il Polo Strategico Nazionale

Le minacce cibernetiche rappresentano, ormai, un rischio estremamente serio per governi, pubbliche amministrazioni, aziende e cittadini. Gli esiti degli attacchi nel 2020 hanno avuto una rilevanza del 56% con impatto alto e critico. I settori maggiormente colpiti sono il settore governativo, quello militare, delle forze dell'ordine e dell'intelligence, oltre a quelli della sanità, della ricerca, dell'istruzione e i servizi online. Inoltre, sono cresciuti gli attacchi verso banking e finance, produttori di tecnologie Hardware e Software e infrastrutture critiche[139]. Relativamente agli attacchi verso istituzioni pubbliche e governi, un cenno va fatto alla Regione Lazio che ha subito un attacco hacker il 1° agosto 2021, attraverso un ransomware, ovvero un codice che si installa nel computer nel momento in cui viene scaricato un file infetto. Un semplice

137 Italia quarta al mondo per cyber minacce legate a pandemia, 16 settembre 2021, su Ansa, consultabile al seguente link: https://www.ansa.it/sito/notizie/tecnologia/hitech/2021/09/16/italia-quarta-al-mondo-per-cyber-minacce-legate-a-pandemia_03631d75-a9cb-4bb2-8a92-4bd1b23644f7.html
138 "Void Balaur: chi è e come agisce la gang criminale che da cinque anni spia tutto il mondo", consultabile al seguente link: https://www.cybersecurity360.it/nuove-minacce/void-balaur-chi-e-e-come-agisce-la-gang-criminale-che-da-cinque-anni-spia-tutto-il-mondo/
139 Cit. PAOLO TARSITANO, Rapporto Clusit 2021: +14% di attacchi di spionaggio cyber, nel mirino i vaccini Covid-19, 2 marzo 2021, consultabile al seguente link: https://www.cybersecurity360.it/nuove-minacce/rapporto-clusit-2021-14-di-attacchi-di-spionaggio-cyber-nel-mirino-i-vaccini-covid-19/

clic su un allegato di una mail ha fatto scaricare un malware che ha potuto cominciare il suo lavoro di crittografia dati. Per evitare la perdita dei dati sanitari di 5,8 milioni di persone, il sistema di erogazione dei servizi informatici è stato temporaneamente bloccato, compreso quello per la gestione della campagna vaccinale. La polizia postale e il centro nazionale anticrimine stanno indagando per risalire al gruppo di criminali che ha sferrato l'attacco informatico, anche se il presidente Nicola Zingaretti ha smentito che è stato richiesto un riscatto in bitcoin[140]. L'accaduto dovrebbe far riflettere non solo l'opinione pubblica e la politica, ma le istituzioni, in quanto risultano essere necessari e improcrastinabili investimenti su software all'avanguardia che proteggano le istituzioni da questi attacchi, oltre un investimento sulla formazione e cultura su tali temi dei dipendenti, al fine da ridurre al minimo i rischi derivanti da attacchi esterni. L'Italia in tal senso ha fatto un annuncio relativamente alla strategia del cloud computing nel settore pubblico, con l'obiettivo di far migrare tutti i dati della pubblica amministrazione entro il 2025 su un cloud, con un investimento pari a 2 miliardi di euro. La strategia applica il principio del cloud first, favorendo l'adozione da parte delle Pubbliche Amministrazioni di strumenti e tecnologie di tipo cloud nello sviluppo di nuovi servizi e nell'acquisizioni di software. L'utilizzo di tali servizi cloud può avvenire solo se questi ultimi risultino qualificati e quindi abbiano quei requisiti di sicurezza, affidabilità, e scalabilità volti a migliorare il livello dello stesso. Per realizzare il consolidamento e la messa in sicurezza delle infrastrutture digitali della PA, l'art.35 del D.L. 76/2020 (semplificazioni e innovazione digitale) modificando l'art. 33-septies del D.L. 179/2012 (ulteriori misure urgenti per la crescita del Paese), ha introdotto la realizzazione di una infrastruttura ad alta affidabilità (detta anche Polo Strategico Nazionale) localizzato sul territorio nazionale promosso dalla Presidenza del Consiglio dei Ministri, attraverso il Dipartimento per la trasformazione digitale con il supporto dell'Agenzia per la cybersicurezza nazionale[141].

5. Sicurezza e insicurezza digitale, verso una nuova alfabetizzazione.

La percezione del rischio informatico è spesso sottostimata soprattutto da eventi avversi, in quanto molti sono ancora analfabeti digitali. La cybersecurity gioca un ruolo

[140] "Attacco hacker alla Regione Lazio: dubbi sul riscatto e preoccupazione per i vaccini", 8 agosto 2021, consultabile al seguente link: https://www.agi.it/cronaca/news/2021-08-08/arracco-hacker-dubbi-riscatto-13518843/

[141] "La Strategia Cloud Italia", consultabile al seguente link: https://cloud.italia.it/strategia-cloud-pa/

fondamentale sull'alfabetizzazione digitale di tutti noi, oltre un ruolo fondamentale nella svolta etica nella fase di progettazione delle piattaforme online. Questo sottostimare gli eventi digitali avversi non appartiene solo a noi comuni cittadini, ma anche a persone con ruoli istituzionali più importanti e, infatti, basti ricordare come un hacker dopo cinque tentativi è riuscito a decifrare la password dell'account twitter di Donald Trump, che si celava sotto il nome di maga2020, ovvero lo slogan del Presidente, "make america great again". Tanti di noi sono soliti utilizzare tipologie di password facilmente hackerabili o sempre le stesse password per dispositivi o siti diversi. Questo utilizzo incauto degli strumenti informatici potrebbe recarci danni senza che noi ce ne rendiamo conto. Sul punto, infatti, basti pensare che Alexa dovrebbe essere utilizzata senza che poi possa ascoltare le nostre conversazioni, o che andrebbe evitato l'invio di foto di soggetti minori attraverso piattaforme di messaggistica come Whatsapp e Facebook. Il problema come sempre è la percezione del rischio e infatti il rapporto costi/benefici è strettamente correlato al modo in cui percepiamo e analizziamo la situazione pericolosa. Nel 1738 Bernoulli aveva teorizzato l'approccio psicofisico all'approccio decisionale, sottolineando un'avversità al rischio, quindi preferendo una sicurezza minore a un azzardo incerto. Le nostre decisioni quindi si muovono in base al concetto di percezione che prescinde dal rischio oggettivo, ma si basa su valutazioni soggettive. La nostra percezione del rischio avverrà attraverso quella che è chiamata la teoria del doppio processo che differenzia il rischio terrificante da quello sconosciuto. In base a queste due possibilità, ciascuno di noi farà una sua mappa cognitiva del rischio e quindi se una condivisione porterà per noi più benefici che rischi allora lo stesso rischio verrà percepito come limitato o meno grave. Infatti, procrastinando monitoraggi, controlli, utilizzo di password adeguate, saremo impreparati ad un eventuale attacco informatico da parte di hacker. La mente umana cerca di ottimizzare i propri pensieri proprio per allontanare lo stress e pertanto in caso di attacco farà il cosiddetto errore di attribuzione, cercando quindi di trovare sempre un capro espiatorio, come un hacker troppo preparato anche per normali sistemi di protezione. Questo può anche accadere in persone esperte che, avendo un controllo personale del rischio, hanno l'idea di gestire la situazione avversa. Attesa l'analfabetizzazione digitale e come il rischio sia un processo soggettivo che più delle volte discosta dalla realtà oggettiva, è di vitale importanza compiere quei passi nella direzione dell'alfabetizzazione di tutti gli utenti, al fine di rendere meno distante la percezione soggettiva da quella

oggettiva e quindi aumentare una sensibilizzazione al rischio, al fine di ridurre le situazioni pericolose[142]. L'alfabetizzazione digitale è necessaria, oltre che per la prevenzione dei rischi, anche per realizzare una vera cittadinanza digitale che parte dalla cultura e dall'utilizzo pratico degli strumenti digitali. L'Italia, in tal senso, si colloca al ventottesimo posto in materia di Competenze Digitali, cioè all'ultimo posto degli Stati membri dell'Unione Europea. Il Piano operativo della strategia nazionale per le competenze digitali rappresenta un'importante azione che dovrebbe portare l'Italia entro il 2025 al pari di nazioni come la Germania, la Francia e la Spagna. Questo piano nasce dalla volontà del dipartimento per la trasformazione digitale del Ministero per l'innovazione tecnologica e la transizione digitale, ha l'obiettivo di combattere il divario digitale di carattere culturale presente nella popolazione italiana, al fine di sostenere una inclusione informatica e favorire l'educazione sulle tecnologie del futuro. Il Piano si propone di raggiungere entro il 2025 l'alfabetizzazione digitale di almeno il 70% della popolazione, duplicare la popolazione in possesso di competenze digitali avanzate, triplicare il numero di laureati in ICT, aumentare di cinque volte il numero della popolazione che utilizza servizi digitali pubblici. Anche se il piano rappresenta un'importante strategia per aumentare l'alfabetizzazione non risultano sufficienti le azioni rivolte a quella parte di popolazione più svantaggiata che ha basso livello di istruzione o agli adulti over 65 con competenze digitali nulle o solo di base. La proposta contenuta nel piano è quella di creare presidi, nodi di facilitazione, presenti su tutto il territorio nazionale che possano supportare e agevolare il cittadino nell'uso delle tecnologie informatiche e nell'accompagnamento degli stessi all'utilizzo dei servizi pubblici digitali. Per facilitare l'utilizzo delle nuove tecnologie sarà predisposto anche la figura del facilitatore digitale, una figura funzionale nell'utilizzo dei servizi digitali e di internet e tale da fornire agli utenti supporto e orientamento. Nel maggio 2021 è stato avviato in forma sperimentale il "Servizio Civile Digitale", incluso anche nel PNRR, come una delle azioni del Piano operativo della strategia nazionale, al fine di poter permettere alla popolazione l'utilizzo dei servizi pubblici online e diffondere un approccio consapevole dell'attuale realtà digitale. Il compito prefissato dall'Italia non è semplice ma è di vitale importanza, per far si che il Paese risalga nella classifica

[142] Cit. DARIA GRIMALDI, Cybersecurity alla sfida cognitivista, ecco i bias che ci rendono "insicuri digitali", consultabile al seguente link: https://www.agendadigitale.eu/sicurezza/privacy/cybersecurity-alla-sfida-cognitivista-ecco-i-bias-che-ci-rendono-insicuri-digitali/

dell'alfabetizzazione digitale, con un ampliamento delle competenze sia di base che specialistiche dell'intera popolazione, al fine di rendere la popolazione italiana tra le più digitalizzate[143]. Ancora molti sono i passi da compiere, ma la strada sembrerebbe quella giusta, per far si che anche la popolazione italiana sia pronta alla transizione digitale, ormai già da qualche anno iniziata anche in altri Paesi.

[143] Cit. DOMENICO LAFORENZA, "Alfabetizzazione digitale, dopo il covid è necessaria: ecco perché", link: https://www.agendadigitale.eu/cittadinanza-digitale/alfabetizzazione-digitale-dopo-il-covid-e-necessaria-ecco-perche/

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*

This work is published under a Creative Commons Attribution-NonCommercial-No-Derivatives 4.0 International License (CC BY-NC-ND 4.0). You may freely download it but you must give appropriate credit to the authors of the work and its publisher, you may not use the material for commercial purposes, and you may not distribute the work arising from the transformation of the present work.

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it