Rivista Semestrale

Luglio - Dicembre 2022

N. 2/2022

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

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.

DATI PERSONALI COME MONETA DI SCAMBIO PER LE PRESTAZIONI RESE NELL'AMBITO DEI MERCATI DIGITALI

Di Chiara Rosa Cerrone

Abstract: *The main aim of this paper is to show how big data are linked with competition world. Nowdays, big data are the money to avail of certain services provided by digital platforms that use user data for commercial purposes. From this point of view users become consumers and this allows to apply consumer discipline. This is what the Authorities (especially the Italian Competition Authority) highlighted, how it happened in Facebook case, in which according Italian Competition Authority and then Italian Administrative Judges the social network has realized unfair business practices. To reduce such phenomena, it is important that consumers understand that their personal information i sas valuable as money.*

1. Introduzione.

Molti credono che i Big Data e il diritto della concorrenza siano due universi distinti e tra loro contrapposti, ma così non è. Come dimostrato dall'indagine congiuntamente svolta dall'Autorità Garante della Concorrenza e del Mercato (AGCM), dall'Autorità Garante per le Comunicazioni (AGCOM) e dal Garante per la Protezione dei Dati Personali (GPDP), e come si cercherà di dimostrare in questo contributo, al diritto della privacy e dell'informazione è possibile approcciarsi ponendosi dalla prospettiva della tutela del consumatore.

Il 30 maggio 2017 l'Autorità per le garanzie nelle comunicazioni ("AGCOM"), con delibera n. 217/17/CONS recante "Avvio di un'indagine conoscitiva sui Big Data", l'Autorità garante della concorrenza e del mercato ("AGCM"), con provvedimento n. 26620 del 30 maggio 2017 "IC53 – Big Data", e il Garante per la protezione dei dati personali, sulla base delle determinazioni adottate nell'adunanza collegiale

dell'11 maggio 2017, hanno avviato un'indagine comune per approfondire gli effetti prodotti dal fenomeno della circolazione dei Big Data e per analizzarne le conseguenze in relazione all'attuale contesto economico e politico-sociale, entro il quadro della regolamentazione in vigore.

Per quanto concerne - più nello specifico - l'indagine condotta dall'AGCM, essa lambisce ciascuno degli ambiti in cui si articola il diritto della concorrenza, e cioè: i) le intese restrittive della concorrenza[1] in relazione al legame tra algoritmi di prezzo e collusione tacita; ii) il controllo delle concentrazioni[2] , con analisi e valutazioni sulle soglie di notifica e sul parametro dell'impedimento significativo della concorrenza effettiva (Substantial impediment to effective competition - SIEC[3]) e iii) gli abusi di posizione dominante[4], mediante l'individuazione di alcune strategie "tipiche".

[1] L'art. 2 della legge 287/1990 - recante norme a tutela della concorrenza e del mercato - vieta gli accordi tra imprese che hanno ad oggetto o per effetto quello di impedire, restringere o falsare in maniera consistente il gioco della concorrenza. Per esempio, ciò accade allorquando più imprese fissano congiuntamente i prezzi o si spartiscono i mercati oppure quando più imprese, che rappresentano una consistente parte del mercato, sottoscrivono una pluralità di accordi distributivi in esclusiva, tali da pregiudicare la capacità di accesso al mercato dei propri concorrenti attuali o potenziali. Si tratta dunque di quelle ipotesi in cui le imprese, piuttosto che competere tra di loro, si accordano al fine di coordinare i propri comportamenti sul mercato. La norma italiana rispecchia la disciplina comunitaria (articolo 101 del Trattato sul funzionamento dell'Unione europea); infatti, se le intese sono idonee a pregiudicare il commercio tra gli Stati membri, l'Autorità antitrust è tenuta ad applicare la normativa comunitaria.

[2] Un'impresa può crescere concentrandosi con altre imprese, fondendosi o acquisendone il controllo, cioè esercitando un'influenza determinante su un'altra impresa (Art. 7 legge n. 287/1990). Si ha, inoltre, un'operazione di concentrazione quando due o più imprese procedono alla creazione di un'impresa comune che esercita stabilmente tutte le funzioni di un'entità economica autonoma (Art. 5 legge n. 287/1990). Le operazioni di concentrazione potrebbero compromettere il gioco della concorrenza, giacchè potrebbero consentire alla nuova entità di aumentare i prezzi o praticare condizioni svantaggiose per le controparti. È per tale ragione che tali operazioni devono essere preventivamente comunicate all'AGCM (Art.16 legge n.287/90) quando il fatturato totale, realizzato a livello nazionale dall'insieme delle imprese interessate, e il fatturato totale realizzato individualmente a livello nazionale da almeno due delle imprese interessate, superino determinate soglie, aggiornate dall'Autorità annualmente, sempre che non ricorrano le condizioni perché la concentrazione ricada nella competenza della Commissione UE. Allorquando vi sia un potenziale rischio per la concorrenza, la concentrazione non viene negata *sic et simpliciter*, ma può essere comunque autorizzata al rispetto di determinate condizioni.

[3] Si tratta di un nuovo criterio impiegato per valutare se una determinata concentrazione sia lesiva della concorrenza, per cui una concentrazione è vietata solo se impedisce sostanzialmente la concorrenza effettiva e non se comporta anche una posizione dominante sul mercato.

[4] Un'impresa detiene una posizione dominante quando può comportarsi in modo significativamente indipendente dai concorrenti, dai fornitori e dai consumatori. In genere ciò avviene quando detiene quote elevate in un determinato mercato. La legge non vieta la posizione dominante in quanto tale, ma il suo abuso (articolo 3 della legge n. 287/1990), che si concretizza quando l'impresa sfrutta il proprio potere a danno dei consumatori ovvero impedisce ai concorrenti di operare sul mercato, causando, conseguentemente, un danno ai consumatori. Alla stessa stregua di quanto previsto per le intese, quando l'abuso determina un pregiudizio per il commercio tra più Stati membri dell'UE, l'Autorità applica la normativa comunitaria (articolo 102 del Trattato sul funzionamento dell'Unione Europea).

Da quest'approccio multidisciplinare posto in essere da queste tre distinte Autorità sono venute alla luce le caratteristiche economiche delle piattaforme digitali, nonchè l'importanza che per esse ha l'acquisizione dei c.d. big data che, come si vedrà, fungono da moneta di scambio per la fruizione di prestazioni offerte senza un corrispettivo monetario strettamente inteso. Proprio tale ultimo aspetto incide in maniera rilevante sul comportamento dei consumatori che sovente si trovano a compiere scelte irrazionali e inconsapevoli.

A scanso di equivoci, è bene sottolineare sin da subito, che le violazioni della privacy e dei diritti dei consumatori di cui qui si discorre, non costituiscono illeciti antitrust, ma rientrano nella fattispecie delle pratiche commerciali scorrette. Paradigmatico in tal senso è il caso – ivi analizzato – del colosso dei social network Facebook, la cui condotta è stata pesantemente sanzionata dall'AGCM.

Per garantire il benessere dell'utente/consumatore, è necessario incrementare l'equità e la trasparenza delle interazioni commerciali che si consumano nei mercati dei c.d. servizi digitali, ove si svolgono attività economiche tutte diverse tra loro ma collegate dalla circostanza che si realizzano attraverso la rete internet (e.g., motori di ricerca, marketplaces, social network, ecc.).

Il precipuo scopo di tale scritto è far comprendere che l'acconsentire al trattamento dei dati personali – attraverso strumenti rapidi ma problematici come quello delle "terms and conditions" - può rivelarsi rischioso non soltanto dal punto di vista della privacy, ma altresì da quello – da molti non preso in considerazione – della tutela del consumatore, il quale diviene preda facilmente catturabile attraverso l'utilizzo di pratiche commerciali scorrette, e dunque mediante l'inserimento – da parte dell'imprenditore – di cunei di ingannevolezza o aggressività nei rapporti commerciali.

2. Alcuni brevi cenni sulle pratiche commerciali scorrette.

Il tecnicismo che contraddistingue la materia del diritto della concorrenza e della tutela del consumatore impone una preliminare disamina sulla disciplina consumeristica, che si rivelerà utile per comprendere i casi pratici analizzati più avanti.

La normativa di riferimento in materia di tutela del consumatore è costituita dal codice del consumo (D.lgs. n. 206/2005), da ultimo modificato con la legge 24 dicembre 2007 n. 244, che ha introdotto per i consumatori la possibilità di esperire la c.d.

"azione di classe", prevista dall'art. 140-bis del Codice del Consumo; tale azione consente ad una pluralità di consumatori danneggiati dal medesimo soggetto di tutelare i propri diritti in maniera collettiva.

Orbene, per ciò che qui interessa, va anzitutto ricordato che l'art. 5 del D.lgs. n. 206/2005 sancisce un obbligo generale – gravante sul professionista – di informare il consumatore sulla sicurezza, composizione e qualità dei prodotti. Il terzo comma dell'articolo 5 del Codice del Consumo surrichiamato specifica i requisiti che devono essere rispettati nell'adempimento di tale obbligo, prevedendo in particolare che le informazioni al consumatore devono essere: a) conformi alla tecnica utilizzata per diffonderle; b) espresse in modo chiaro e comprensibile per un consumatore medio, ed in particolare non devono essere fuorvianti, anche in considerazione delle modalità di conclusione del contratto o delle caratteristiche del contratto stesso; c) tali da assicurare la consapevolezza del consumatore. E' dunque necessario che quest'ultimo sia posto nella condizione di riconoscere le caratteristiche del prodotto o del servizio offerto, per poter fare una scelta veramente consapevole tra prodotti concorrenti, nonché utilizzare quanto acquistato con sicurezza ed in modo soddisfacente e, infine, poter ricevere tutela dei propri diritti in caso di danno derivante dall'acquisto del prodotto o del servizio.

Se un'impresa tenta di falsare le scelte economiche del consumatore, per esempio omettendo informazioni rilevanti o diffondendo informazioni non veritiere, pone in essere – violando gli obblighi informativi sopraricordati – una pratica commerciale scorretta, di fronte alla quale l'Antitrust[5] può intervenire anche in via cautelare, stigmatizzando la condotta con l'irrogazione di sanzioni anche piuttosto pesanti.

Per pratica commerciale si intende ogni azione, omissione, condotta, dichiarazione o comunicazione commerciale, ivi compresa la pubblicità diffusa con ogni mezzo (incluso il direct marketing e la confezione dei prodotti) e il marketing, che un professionista pone in essere per promuovere, vendere o fornire beni e/o servizi ai consumatori.

Il Codice del Consumo (artt. 18-27 quater) vieta le pratiche commerciali scorrette che, in contrasto con il principio della diligenza professionale (ossia il normale grado della specifica competenza ed attenzione che i consumatori possono ragionevol-

[5] Autorità Garante della Concorrenza e del Mercato (AGCM).

mente attendersi da un professionista nei loro confronti, nel rispetto dei principi generali di correttezza e di buona fede nell'ambito dell'attività del professionista) falsano o sono idonee a falsare in misura apprezzabile il comportamento economico del consumatore medio che raggiungono o al quale sono dirette. Ciò che si intende salvaguardare è la libertà di scelta del consumatore, affinchè non sia indotto a prendere decisioni di natura economica che altrimenti non avrebbe preso. La normativa di riferimento le distingue in ingannevoli ed aggressive; le prime, di cui agli articoli 21-23 del Codice del Consumo, sono idonee ad indurre in errore il consumatore, falsando quegli elementi principali di cui egli tiene conto nel processo decisionale, quali il prezzo, la disponibilità sul mercato del prodotto, le sue caratteristiche, i rischi connessi al suo impiego, e così via. L'Autorità Garante della Concorrenza e del Mercato considera illecite altresì "le pratiche che inducono il consumatore a trascurare le normali regole di prudenza o vigilanza in relazione all'uso di prodotti pericolosi per la salute e la sicurezza o che possano - anche indirettamente - minacciare la sicurezza di bambini o adolescenti". Le pratiche si dicono invece aggressive – ai sensi degli artt. 24-26 del Codice del Consumo - allorquando l'impresa agisce con molestie, coercizione o altre forme di indebito condizionamento.

Gli articoli 23 e 26 del Codice del Consumo indicano pratiche che in ogni caso devono considerarsi scorrette, rispetto alle quali dunque non è ammessa prova contraria. Si tratta delle c.d. "black lists" (liste nere), ossia un elenco di pratiche la cui illiceità viene determinata a monte dal legislatore, a prescindere da ogni valutazione del caso in concreto.

Per esempio, sono in ogni caso ingannevoli – ai sensi dell'art. 23 lettera f) Codice del Consumo - quelle pratiche che invitano ad acquistare prodotti ad un determinato prezzo e successivamente, 1) la dimostrazione dell'articolo viene fatta con un campione difettoso, con l'intenzione di promuovere un altro prodotto, oppure, quando ci si rifiuta di: 2) mostrare l'articolo pubblicizzato ai consumatori oppure 3) di accettare ordini per l'articolo o di consegnarlo entro un periodo di tempo ragionevole. Ancora, ai sensi della lettera g) dell'art. 23 del Codice del Consumo, è in ogni caso ingannevole la pratica con la quale si dichiara, contrariamente al vero, che il prodotto sarà disponibile solo per un periodo molto limitato o che sarà disponibile solo a condizioni particolari per un periodo di tempo molto limitato, così da ottenere una decisione immediata dei consumatori, che vengono in questo modo privati della possibilità o del tempo sufficiente per prendere una decisione consapevole.

L'elenco delle pratiche "in ogni caso aggressive" è invece contenuto nell'articolo 26 del Codice del Consumo, il quale alla lettera a) considera – per esempio - come aggressiva, la pratica che porta ad ingenerare nel consumatore l'impressione che egli non possa lasciare i locali commerciali fino alla conclusione del contratto, o ancora, effettuare ripetute e non richieste sollecitazioni commerciali per telefono, via fax, per posta elettronica o altro mezzo di comunicazione a distanza, al di fuori dei casi previsti dalla legge (art. 26 lett. c) del Codice del Consumo).

Quando un professionista pone in essere una pratica commerciale scorretta, interviene l'Autorità Garante della Concorrenza e del Mercato che, d'ufficio o su istanza di ogni soggetto o organizzazione che ne abbia interesse, inibisce la continuazione di tali pratiche, eliminandone gli effetti, nonchè applicando le sanzioni amministrative previste dall'art. 27 del D.lgs. n. 146 del 2007.

Laddove il professionista si impegni a porre fine all'infrazione o a modificare la pratica sleale (così da eliminare ogni profilo di illegittimità), l'AGCM, dopo aver valutato l'idoneità di tale impegno, può renderlo obbligatorio, disponendo la pubblicazione della dichiarazione del professionista (a sue spese) e definendo in questo modo il procedimento senza proseguire verso l'accertamento dell'illecito.

In ogni caso, quando si dia avvio all'istruttoria, il professionista interessato deve essere messo a conoscenza di ciò e, ove mai questi non sia conosciuto, l'Autorità può richiedere informazioni sulla sua identità al proprietario del mezzo di comunicazione che ha diffuso la pratica commerciale.

In merito alle prove, l'articolo 27 del D.lgs. n. 146 del 2007 soprarichiamato prevede, innanzitutto, che l'AGCM può richiedere a qualsiasi soggetto che ne sia in possesso, le informazioni ed i documenti rilevanti per l'accertamento della pratica sleale. La norma prevede altresì che, in ragione delle esigenze connesse al caso specifico, nel corso del procedimento l'onore della prova può essere invertito, nel senso che dovrà essere il professionista – e non il denunciante – a fornire le prove degli elementi materiali comprovanti la realizzazione della pratica contestata; a condizione che ciò non leda i diritti e gli interessi legittimi dell'imprenditore o di qualsiasi altra parte del procedimento. In caso di omissione della prova richiesta, o qualora questa dovesse essere ritenuta insufficiente, le circostanze fattuali addotte dovranno considerarsi inesatte e la pratica commerciale, scorretta (art. 27 comma 5 D.lgs. n. 146 del 2007).

La decisione finale dell'Antitrust è suscettibile di contestazione, con ricorso al Giudice Amministrativo. E' però fatta salva la giurisdizione del giudice ordinario, che

sussiste laddove la pratica posta in essere integri un atto di concorrenza sleale di cui all'articolo 2598 del codice civile, o quando con essa venga violata la disciplina del diritto di autore (Legge n. 633/1941 e successive modificazioni), o quella concernente il marchio di impresa (D.Lgs. n. 30/2005) o, infine, quella delle denominazioni di origine riconosciute e protette in Italia e di altri segni distintivi di imprese, beni e servizi concorrenti.

3. La dimensione economica dei dati personali.

Generalmente, la materia dei dati personali viene analizzata sotto un'ottica di tipo strettamente personalistico. Tale approccio è frutto della definizione stessa di "dato personale", inteso come informazione che identifica o rende identificabile una data persona fisica; è un dato personale perché appunto riferito alla persona, e perciò tutelabile alla stregua dell'art. 2 Cost. che garantisce "i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità".

Senonchè, non considerare l'aspetto anche patrimoniale delle informazioni personali degli individui si risolverebbe in una mistificazione. Da tale angolo visuale, merita menzione una recentissima sentenza del Consiglio di Stato (Cons. St. 29 marzo 2021 n. 2631) che ha proprio messo in evidenza la "commerciabilità" del dato personale, consentendo – in siffatto modo – di riconoscere tutele di natura patrimoniale anche quando in gioco vi siano questioni che - solo apparentemente - non hanno nulla da spartire con la logica commercialistica e con lo scambio economicamente inteso. Il caso de quo su cui si sono espressi i giudici di Palazzo Spada, dimostra come i dati personali forniti da una persona possano costituire il corrispettivo per la prestazione di servizi solo in apparenza gratuiti. L'errore in cui solitamente si incorre è credere che la mancanza di un "prezzo", così come comunemente viene inteso, ossia come esborso monetario reso a fronte di un bene o di un servizio, permette di imprimere carattere gratuito alla prestazione che ci viene resa, per la quale, a ben vedere, il costo è rappresentato da noi stessi e dal nostro universo di informazioni private. Tale meccanismo può essere facilmente compreso se si pensa alle piattaforme digitali che forniscono prestazioni che sembrano appunto essere gratuite, ma che invero richiedono come corrispettivo la condivisione di dati strettamente personali, quali l'età, l'indirizzo di casa, dati sulla posizione, e così via. La presunta gratuità di quanto ci viene reso è conseguenza della libertà che ha l'utente/consumatore di scegliere quali informazioni condividere. Tale punto viene messo bene in evidenza nella decisione soprarichiamata che

fa luce sulla patrimonializzazione[6] che questi dati subiscono quando si sottoscrive un accordo con i c.d. social network. I dati che vengono richiesti al momento dell'iscrizione fungono da materie prime che vengono inserite in un circuito produttivo basato proprio sullo sfruttamento delle informazioni personali, utilizzate per creare spazi pubblicitari mirati e "ad personam", si potrebbe dire. I dati vengono così immessi nel mercato, che gli imprime "un valore di uso e un valore di scambio, li assurge a beni economici e, quindi, a beni giuridici, disponendoli così alla contrattualizzazione" [7].

A ben vedere dunque, ancorchè molti dei servizi offerti dalla rete siano definiti "free of monetary charge" [8], il "carico" è invece costituito dai dati personali, che nei mercati digitali fungono da vera e propria merce di scambio[9]. Per essere più precisi, i dati forniti dall'utente/consumatore non sono strettamente necessari all'esecuzione del contratto sottoscritto con il gestore della piattaforma; piuttosto, servono a quest'ultima per immetterli in un processo di profilazione necessario per raggiungere determinati fini commerciali, e cioè incrementare la vendita di determinati beni e/o servizi, attraverso una pubblicità più mirata, che si confaccia alle caratteristiche proprie dell'utente. Paradigmatico, in tal senso, è quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 per la protezione dei dati personali ("GDPR"), attuato in Italia con il d.lgs. 19 agosto 2018 n. 101, che - all'art. 7 par. 4 – tiene in conto la ormai comune ipotesi della prestazione di un servizio "condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

E' bene però precisare che il rapporto tra piattaforma digitale ed utente è pur sempre caratterizzato dal carattere della sinallagmaticità, come messo in luce dalla

[6] Per un'analisi più completa del fenomeno della patrimonializzazione si vedano R. Senigaglia, La dimensione patrimoniale del diritto alla protezione dei dati personali, in Contr. impr., 2020, 760 ss.; V. Ricciuto, Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati, in Riv. dir. civ., 2020, 642; Id., La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, in Dir. inform., 2018, 689; A. De Franceschi, La circolazione dei dati personali tra privacy e contratto, Napoli, 2017; S. Thobani, Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali, Milano, 2018.
[7] R. Senigaglia, La dimensione patrimoniale del diritto alla protezione dei dati personali, cit., 2020, 765.
[8] Espressione utilizzata dall'Autorità Garante della Concorrenza e del Mercato italiana nel provvedimento n. 27432 del 29 novembre 2018, concernente le pratiche commerciali scorrette poste in essere da Facebook.
[9] Questa impostazione trova riscontro nella Direttiva (UE) 2019/770 sulla fornitura di servizi e contenuti digitali. In particolare, nell'art. 3, comma 1 (dedicato all'ambito di applicazione della Direttiva) si stabilisce che: "*la presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico*".

giurisprudenza unionale. La Corte di Giustizia dell'Unione europea[10] infatti, ha espressamente riconosciuto che l'attività posta in essere da un soggetto digitale che offre un bene o un servizio a prezzo apparentemente nullo, ha natura economica. Invero, la presunta mancanza del prezzo viene sopperita con i finanziamenti ottenuti tramite la pubblicità, per la quale un ruolo assolutamente importante è assolto dai dati personali degli utenti.

Orbene, la natura patrimoniale dei dati personali e dunque l'esistenza di uno scambio insito nella prestazione/fruizione dei servizi digitali apparentemente gratuiti, pone in capo al fornitore digitale "uno specifico obbligo informativo nei confronti del consumatore rispetto all'utilizzo dei dati personali da questi messi a disposizioni per finalità di profilazione". Va pertanto seguita quella "più attenta e, tuttavia, ancora ad oggi minoritaria dottrina[11]" che, svincolando il concetto di atto dispositivo dal "paradigma della cessione traslativa[12]", supera l'ormai consolidata concezione del dato personale - quale attributo della persona - che si incentrata esclusivamente sulla personalità del soggetto a cui si riferisce.

In siffatto modo il dato personale, lungi dal costituire soltanto - ed in maniera esclusiva - l'oggetto di un diritto fondamentale dell'individuo, e in quanto tale tutelabile soltanto in tale contesto, diviene oggetto scambiabile e negoziabile, suscettibile di essere sfruttato economicamente.

Tuttavia, nell'ambito europeo si sono levate voci contrarie al riconoscimento della dimensione anche patrimoniale del dato personale, giacchè si dice che se quest'ultimo venisse inteso come "corrispettivo non pecuniario", verrebbe svilito del proprio senso, del proprio essere diritto fondamentale della persona. In particolare, in questi termini si è espresso il Garante europeo della protezione dei dati personali[13], nonché il comitato europeo per la protezione dei dati (European Data Protection Board,

[10] Corte di Giustizia dell'Unione europea, 26 aprile 1988, Bond van Adverteerders e altri c. Paesi Bassi, C-352/85, punti 16-17.
[11] B. Parenzo, "*Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti"*, in Diritto di Famiglia e delle Persone (Il), fasc.3, 1.09.2021, pag. 1457.
[12] Ibid.
[13] Opinion n. 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, nella quale si incoraggia ad evitare di considerare i dati personali come controprestazione: "*personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity*".

"EDPB" [14]) che nelle linee guida n. 2/2019 concernenti il trattamento dei dati personali svolto ex art. 6, par. 1 lett b), GDPR, ha preliminarmente ricordato che il diritto alla protezione dei dati personali è un diritto fondamentale garantito dall'art. 8 della Carta europea dei diritti fondamentali, sottolineando poi che i dati personali non possono essere considerati merci commerciabili; pertanto, gli interessati possono acconsentire al trattamento dei propri dati, senza tuttavia poterne disporre, in quanto loro diritti fondamentali.

Senonchè, con il riconoscimento della dimensione economica dei dati personali, la loro tutela non viene stigmatizzata, quanto piuttosto ampliata. Difatti, il processo di "patrimonializzazione" a cui vengono sottoposte le informazioni personali che ciascun utente fornisce nell'ambito delle proprie interazioni con gli operatori dei mercati digitali, disvelando l'altra faccia del cliente digitale (quella consumeristica), impone il rispetto – anche nell'ambito di tali transazioni commerciali – di *"quegli obblighi di chiarezza, completezza, e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore che deve essere edotto dello scambio di prestazioni che è sotteso all'adesione ad un contratto per la fruizione di un servizio*" digitale, come può essere quello dell'utilizzo di un social network. Dare ossequio a tali obblighi è molto importante, giacchè consente di arginare il possibile vulnus che può subire la sfera del consumatore e, più in generale, consente di evitare le sempre possibili distorsioni della concorrenza; posto che il dato personale da mera "*informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica*[15] " diviene un bene economicamente rilevante che, entrando a far parte dell'assetto patrimoniale di un'impresa, ne accresce la forza concorrenziale nel mercato. A tale ultimo riguardo, è interessante notare come le principali piattaforme digitali competano non - come generalmente accade - nell'ambito di un determinato mercato, ma per più mercati tra loro diversi, accomunati da un modello imprenditoriale incentrato sull'utilizzo della rete e l'analisi dei dati. Dal punto di vista della tutela del consumatore invece, il principale problema che si pone è costituito dalla presenza di asimmetrie informative, stante il ruolo svolto dalle piattaforme digitali, e cioè quello di intermediari che creano interazioni commerciali tra due categorie diverse di soggetti economici (utenti/consu-

[14] Si tratta di un organismo dell'Unione europea, indipendente e dotato di personalità giuridica, che contribuisce alla coerente applicazione delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità di controllo.
[15] Definizione comune di dato personale accolta dal Garante per la Protezione dei Dati Personali.

matori da un lato, e utenti/fornitori dall'altro). Così, per esempio, quando il consumatore si appresta a comprare un prodotto attraverso utilizzando siti di e-commerce, può accadere che manchino adeguate informazioni sulla qualità del prodotto offerto dal rivenditore al dettaglio. La piattaforma potrebbe comunque mitigare – con il suo intervento – i profili problematici che possono all'uopo porsi, ad esempio con l'introduzione di un sistema di recensioni dei prodotti acquistabili. Tuttavia, anche tali soluzioni non risultano essere esenti da problematiche rischiose per il gioco della concorrenza. Si pensi al caso, accaduto[16] nella pratica, in cui la piattaforma mette in rilievo recensioni relative a prodotti di rivenditori che hanno acquistato servizi accessori dalla piattaforma.

La dimensione economica dei dati personali è stata recentemente riconosciuta anche dalla giurisprudenza, che ha infatti messo in evidenza come tali informazioni possano *"costituire un asset disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di controprestazione in senso tecnico di un contratto*[17]", e prima ancora dall'Autorità Garante della Concorrenza e del Mercato ("AGCM") che, riconoscendo il valore economico dei dati degli utenti dei social media, ritiene configurabile anche in questi casi l'esistenza di un rapporto di consumo tra il professionista e l'utente[18]; nonché dalla Commissione europea[19].

Come accennato innanzi, guardare ai dati personali da un punto di vista economico non significa soppiantare l'aspetto personale che per definizione caratterizza tali informazioni che, lungi dall'essere mere informazioni commerciali, sono – occorre ribadirlo - anzitutto e soprattutto elementi che contribuiscono a delineare la personalità e l'identità di una persona. Le due dimensioni (economica e personale) più che prevalere l'una sull'altra si intersecano a vicenda, costituendo un unicum inscindibile sul quale si proietta un sistema articolato di tutele per la persona/consumatore, il "soggetto debole" che merita protezione in questa nuova realtà digitale.

---

[16] Si allude al caso che ha visto pesantemente sanzionato il colosso del web Amazon, per il quale merita però precisare, a scanso di equivoci, che la violazione riscontrata dall'Autorità Garante della Concorrenza e del Mercato non riguardava la tutela del consumatore, quanto piuttosto il diritto della concorrenza strettamente inteso; essendosi rilevata una violazione dell'3 L. 287/1990, nonché dell' art. 102 del Trattato sul Funzionamento dell'Unione europea.
[17] TAR Lazio 10 gennaio 2020 n. 260, in Foro amm.
[18] Così nel provvedimento n. 26596 dell'11 maggio del 2017.
[19] La Commissione negli "Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali" del 25 maggio 2016 ha espressamente asserito che "*i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto e vengono venduti a terzi*".

4. Alcuni esempi pratici: il caso Facebook

Di recente, anche la giurisprudenza ha seguito un approccio negoziale nella protezione dei dati personali, rivelando talaltro le difficoltà incontrate dall'utente nel comprendere le dinamiche di questo meccanismo di patrimonializzazione delle sue informazioni personali che vengono trattate alla stregua di denaro dato in cambio di servizi che in prima *facie*, lo si è detto, sembrano essere gratuiti.

Siffatto orientamento giurisprudenziale si colloca a valle dell'operato svolto dall'Autorità Antitrust italiana che, in buona sostanza, si allinea all'indirizzo intrapreso dalle altre Autorità europee nella salvaguardia della concorrenza nell'ambito dei mercati digitali, ove le imprese si servono dei grandi colossi della rete, i c.d. GAFAM[20] (definiti anche "guardiani" o *gatekeeper* della rete), per raggiungere i consumatori. Nei confronti di questi grandi giganti della rete i Garanti della concorrenza hanno intrapreso un'intensa attività di indagine, sfociata, molto spesso, nell'irrogazione di sanzioni anche piuttosto rilevanti.

La vicenda che ha visto coinvolto il social network Facebook è utile per due ragioni. Anzitutto, mette in risalto la duplice dimensione – personale ed economica – dei dati personali, quali sì informazioni afferenti alla sfera intima delle persone, ma nello stesso tempo moneta di scambio nell'ambito dell'economia digitale. In secondo luogo, essa disvela la mancanza di consapevolezza - da parte dei consumatori - di questo carattere ambivalente dei dati che li riguardano; una manchevolezza beninteso non ad essi imputabile, ma conseguenza delle bulimiche informazioni che gli vengono fornite, talvolta quasi nulle.

Con provvedimento n. 27432 del 29 novembre 2018 l'Autorità Garante della Concorrenza e del Mercato ha pesantemente sanzionato le società "Facebook Inc." e "Facebook Ireland ltd." per aver posto in essere due pratiche commerciali scorrette, in violazione degli artt. 21 e 22, nonché 24 e 25 del Codice del Consumo. La prima va inquadrata nell'ambito delle pratiche c.d. ingannevoli, giacchè Facebook avrebbe indotto in errore gli utenti/consumatori, alterando il loro processo decisionale. Più precisamente, all'iscrizione sulla piattaforma non sarebbe corrisposta un'adeguata informazione circa le finalità commerciali a cui era destinato lo scambio dei propri dati personali. E' lecito immaginare che se avessero avuto più informazioni, molti utenti

[20] Si allude a Google, Amazon, Facebook, Apple, Microsoft.

avrebbero preso una decisione diversa da quella di iscriversi alla piattaforma, presa invece inconsapevolmente, convinti - stante il *claim* utilizzato dalla piattaforma "Iscriviti, è gratis e lo sarà per sempre" - della gratuità della prestazione ricevuta. La seconda pratica presenta invece i connotati delle pratiche commerciali scorrette c.d. aggressive, giacchè i consumatori registrati avrebbero subito un indebito condizionamento, consistente nel trasferimento dei loro dati personali, senza avervi previamente ed espressamente acconsentito. Nello specifico, l'Autorità spiega che, inconsapevolmente e in maniera automatica, tramite un sistema di preselezione del consenso alla cessione e utilizzo dei dati, questi vengono trasferiti a terzi operatori. L'Antitrust ha altresì rilevato che, per evitare di subire limitazioni nell'utilizzo del servizio, gli utenti sarebbero stati indotti – in siffatto modo - a mantenere attivo il trasferimento e l'uso dei propri dati.

In particolare, ciò che va sottolineato, è la qualificazione che l'AGCM ha dato della cessione dei dati, perché intesa come *"contro-prestazione del servizio offerto dal social network, in quanto dotati di valore commerciale*[21]*"*. L'Autorità ha poi fatto notare che dai risultati dell'istruttoria è emerso che il business del gruppo Facebook si basa proprio sulla raccolta e sfruttamento dei dati degli utenti a fini remunerativi. Ciò rende inequivocabile il valore economico assunto dai dati personali, che fungono pertanto da contro-prestazione del servizio offerto dal social network. Si è infatti rilevato che *"i ricavi provenienti dalla pubblicità on line, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd. e il 98% del fatturato di Facebook Inc".* Nel passaggio da ultimo richiamato, si spiega dunque che il patrimonio di dati personali degli utenti di Facebook acquisisce un valore commerciale in ragione dell'uso che se ne fa: tali informazioni vengono utilizzate per fini commerciali e per generali finalità di marketing.

Avverso la decisione dell'AGCM, Facebook Inc. ha presentato ricorso al Tar Lazio che ha negato i profili di aggressività riscontrati dall'Autorità nella seconda condotta posta in essere dal gigante dei *social network*, e ha pertanto annullato parzialmente la sanzione irrogata, per il resto confermata; anche i giudici amministrativi infatti, hanno ravvisato profili ingannevoli della prima condotta assunta da Facebook.

Ciò che vale la pena sottolineare è che il Tar Lazio – alla stessa stregua dell'AGCM – ha riconosciuto il carattere patrimoniale dei dati personali che in questo

[21] Provvedimento n. 27432/2018 § 18.

tipo di scambi commerciali fungono da moneta di scambio; sono cioè idonei ad assurgere al rango di contro-prestazione in senso tecnico di un contratto. Viene dunque riconosciuto il fenomeno della "patrimonializzazione del dato personale", e le parole del tribunale amministrativo sono icastiche al riguardo: *"Le tesi di parte ricorrente presuppongono che l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, e per tale motivo Facebook era tenuta esclusivamente al corretto trattamento dei dati dell'utente ai fini dell'iscrizione e dell'utilizzo del "social network". Tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto".* Il Tar Lazio prosegue il proprio ragionamento chiarendo che alla duplice dimensione – personale ed economica – dei dati personali corrispondono, inevitabilmente, due forme di protezione; l'una incentrata sul concetto di dato personale quale espressione di un diritto della personalità dell'individuo e che si articola in diversi mezzi di protezione quali il diritto di revoca del consenso, di accesso, rettifica, oblio, ecc., l'altra basata sull'aspetto economico del dato personale, che può divenire l'oggetto di una compravendita, e che perciò impone il rispetto della disciplina consumeristica. Più precisamente, secondo i giudici amministrativi la "patrimonializzazione del dato personale", tipica delle nuove economie dei mercati digitali, impone il rispetto – da parte degli operatori – degli obblighi di chiarezza, completezza e non ingannevolezza previsti dalla legislazione posta a tutela del consumatore, affinchè questi possa essere messo nella condizione di fare scelte commerciali consapevoli. Difatti, i profili di illeicità - riscontrati dall'AGCM e poi confermati dal Tar Lazio – della condotta di Facebook, riguardano l'incompletezza delle informazioni fornite all'utente/consumatore, ignaro dei fini commerciali – *rectius* remunerativi – sottesi all'accordo di scambio tra dati personali e utilizzo del social network.

Alla luce di quanto detto, appare chiaro che in capo alle imprese gravano due forme di responsabilità tra loro distinte e concorrenti. Nello specifico, una sorge per violazione della disciplina a tutela della privacy prevista dal Regolamento (UE) 2019/679 e dal D.lgs. 196/2003 con sanzioni fino al 4% del fatturato annuo irrogate dal Garante per la protezione dei dati; l'altra invece è diretta conseguenza della violazione del Codice del Consumo con sanzioni fino a 5 milioni di euro per ogni pratica commerciale accertata dall'AGCM.

I giudici amministrativi hanno poi avuto cura di chiarire che la duplice violazione non crea alcun effetto *"plurisanzionatorio della medesima condotta (intesa come identico fatto storico) posta in essere dal professionista che gestisce il social network".* Secondo il Tar non vi è alcun rischio in tal senso, in quanto l'oggetto di indagine da parte delle competenti autorità Garante dei dati ed AGCM riguarderebbe *"condotte differenti dell'operatore, afferenti nel primo caso al corretto trattamento del dato personale ai fini dell'utilizzo della piattaforma e nel secondo caso alla chiarezza e completezza dell'informazione circa lo sfruttamento del dato ai fini commerciali".*

5. Conclusioni

La praticità del caso Facebook poc'anzi richiamato è molto utile per comprendere concetti forse difficili da intendere, non tanto per la complessità intrinseca degli stessi, quanto piuttosto per la loro teoricità, ma soprattutto perché risulta complicato immaginare che i dati personali, in quanto appunto afferenti alla sfera strettamente personale di un individuo, possono costituire il prezzo per la fruizione di prestazioni, è bene ribadirlo, solo apparentemente gratuite.

E' molto importante – per il consumatore medio - rendersi conto di questa duplice natura del dato personale, giacchè gli consente di arginare il rischio di rimanere invischiato in decisioni palesemente commerciali che altrimenti non avrebbe preso, o quantomeno di difendersi laddove ignaro del valore economico dei propri dati, abbia acconsentito al loro trattamento per fini commerciali.

E' bene altresì ribadire che il carattere multiforme dei dati personali, la multidisciplinarità che li contraddistingue, non fa sorgere alcuna antinomia tra le norme a tutela del consumatore e quelle a tutela del dato personale, inteso dal punto di vista strettamente personalistico. Piuttosto, come ha sottolineato lo stesso Tar Lazio, tali normative "*pongono in termini di complementarietà, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell'altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole*".

Da questa duplicità ne consegue che – nell'ambito del riparto delle competenze tra Autorità Garante della Concorrenza e del Mercato e Garante per la Protezione dei Dati Personali – il primo è competente allorquando i dati personali siano utilizzati per

fini commerciali, e dunque, più precisamente, l'AGCM sarà competente per garantire il rispetto degli obblighi di chiarezza e completezza delle informazioni[22]. La seconda Autorità sarà invece competente in tutti i casi concernenti il corretto trattamento del dato personale nell'utilizzo della piattaforma.

Ancorchè ancora oggi, ad essere privilegiato sia l'approccio morale alla protezione dei dati, la questione della c.d. patrimonializzazione, e dunque dell'aspetto negoziale dei dati personali, era emersa già in passato. Così, per esempio, in occasione dell'entrata in vigore della legge 675/1996 Stefano Rodotà metteva in luce l'esistenza di forme di negoziazione dei dati. Plasticamente, l'insigne giurista faceva notare che: "*Quando si dice che se tu riempi questo questionario riceverai un campione del prodotto, non è un prodotto in omaggio, perché io cedo qualcosa che per il soggetto che mi darà il prodotto ha un valore aggiunto molto maggiore di ciò che mi viene dato, quindi ci sono già delle transazioni economiche su questa base, di difficile definizione, ma certamente ci sono*[23]".

In conclusione, per arginare possibili condotte lesive nei confronti dell'utente digitale che, come visto, diviene anche e soprattutto consumatore, è bene prendere atto del carattere bidimensionale del dato personale, che può pertanto essere analizzato da un duplice punto di vista, morale ed economico; aspetti non necessariamente tra loro antitetici e contrapposti, ma facce di una stessa medaglia.

6. Note Bibliografiche

ALVISI C., *Dati personali e diritti dei consumatori*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), I dati personali nel diritto europeo, Giappichelli, Torino, 2019.

CODICE DEL CONSUMO.

Cons. St. 29 marzo 2021 n. 2631.

Corte di Giustizia dell'Unione europea, 26 aprile 1988, Bond van Adverteerders e altri c. Paesi Bassi, C-352/85, punti 16-17.

[22] C. Alvisi, Dati personali e diritti dei consumatori, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), I dati personali nel diritto europeo, Giappichelli, Torino, 2019, p. 682.
[23] S. Rodotà, Conclusioni, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich, Trattamento dei dati e tutela della persona ripreso da V. Ricciuto, La patrimonializzazione dei dati personali, in Diritto dell'Informazione e dell'Informatica (Il), cit. p. 695.

Opinion n. 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, nella quale si incoraggia ad evitare di considerare i dati personali come controprestazione: *"personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity"*.

PARENZO B., *"Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti",* in Diritto di Famiglia e delle Persone (Il), fasc.3, 1.09.2021.

Provvedimento AGCM n. 26596 dell'11 maggio del 2017.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 per la protezione dei dati personali ("GDPR")

RODOTÀ S., Conclusioni, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich, Trattamento dei dati e tutela della persona ripreso da V. Ricciuto, La patrimonializzazione dei dati personali, in Diritto dell'Informazione e dell'Informatica.

SENIGAGLIA R., *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., 2020, 765.

Tar Lazio, sez. I, 10 gennaio 2020 n. 261.

IL FENOMENO DEL DIGITAL DATING.

DALL'UTILITÀ SOCIALE AI RISCHI PER LA SICUREZZA.

di Tiziana Di Palma

SOMMARIO: 1. Il nuovo modello sociologico dei rapporti affettivi – 2. Condotte di *Catfishing*, *Grooming*, *Romance Scam*, *SexTortion*, *Teen Dating Violence.* Rilievi di diritto penale ed analisi giurisprudenziale – 3. Il *Dating* Digitale e la tutela della privacy. I suggerimenti del Garante *Privacy*.

1. Il nuovo modello sociologico dei rapporti affettivi

Nel cd. villaggio globale, secondo la definizione offerta dal sociologo dei mass media Marshall McLuhan[24], nell'indagine sul progresso tecnologico della società, l'evoluzione della tecnologia appare strettamente legata all'osmosi tra uomo e media, consentendo all'individuo di essere destinatario di plurimi messaggi attraverso la convergenza di TV, PC, telecomunicazioni e favorendo relazioni sempre più immateriali tra gli uomini.

In tale *"non luogo*" (non lieu)[25], si sono sviluppati nuovi modelli di iterazione sociale, suscettibili, altresì, di incidere sulla sfera strettamente personale e di trasformare, conseguentemente, il mondo degli appuntamenti, delle relazioni interpersonali e di condizionare l'ambiente emotivo.

Secondo il sociologo tedesco Simmel, la società si costituisce mediante l'azione reciproca degli individui, affermando che la società è quella somma di relazioni animate da motivi ed interessi, e quindi "*non esiste mai la società in generale nel senso che quei particolari fenomeni di connessione si sono formati soltanto presupponendo la sua esistenza: infatti non esiste alcuna azione reciproca in quanto tale,*

[24] MCLUHAN M., *The Gutenberg galaxy*, 1962, p.31 e MCLUHAN M., POWERS B.R., T*he Global Village: Transformations in World Life and Media in the 21st Century*, New York, Oxford University Press, 1989, p. 31.
[25] AUGÉ M., *Nonluoghi. Introduzione a una antropologia della surmodernità*, Milano Eleuthera, 2009, p. 10.

ma particolari di essa, con cui il manifestarsi la società esiste e che non sono né la sua causa né la conseguenza di questa, ma sono già immediatamente essa stessa"[26].

La società simmeliana implica una riflessione sul concetto ambivalente di identità in quanto la stessa, per esistere, ha bisogno anche del riconoscimento da parte degli altri: gli altri sono costitutivi della nostra identità e dalle "azioni reciproche" degli individui nasce, appunto, la società stessa. Inoltre, la dimensione delle relazioni umane nelle quali un individuo penetra nella vita dell'altro è, per sua natura, esposta allo sconfinamento.

Il tema dei "*confini*" tra l'Io e l'Altro esiste in ogni tipo di relazione e ambiente sociale poiché la questione dell'intimità fa parte della struttura stessa della relazione e assume un significato diverso a seconda delle situazioni in cui si sviluppa la relazione sociale. Se, dunque, oggi con l'avvento dei social media sembra che il discorso emozionale abbia preso il sopravvento al fine di annullare ogni distanza, ogni confine tra l'Io e l'Altro, allora, potrebbe parlarsi di fine della *privacy* e considerarla come una sorta di invenzione postmoderna che serve a coprire un problema più grande, quello della dis-umanizzazione dell'umano.

Viviamo in una società in perenne movimento. Le esperienze individuali e le relazioni sociali si ristrutturano di continuo, in maniera fluida e nomade.

La società liquida[27], in tal senso, è una società dove le tendenze sociali e il potere prendono le distanze dal controllo dell'individuo in quanto le condizioni in cui si muovono le persone cambiano prima ancora che le loro azioni possano stabilizzarsi in prassi comuni. Questo profondo cambiamento, amplificato dall'avvento dei social media, alimenta sempre più una sorta di individualismo esasperato[28].

Tale individualismo, tuttavia, non sembra contrastare con l'intento di stabilire un'interazione all'interno dell'ambiente digitale il quale, agevolando un certo grado di disinibizione, rappresenta il veicolo perfetto per fornire all'interlocutore la "*migliore*" versione di sé e l'occasione di riconfigurare i legami e i rapporti affettivi.

La tecnologia è giunta, dunque, a svolgere un ruolo di potente amplificatore emotivo; le relazioni sentimentali, infatti, nascono, si costruiscono e vengono vissute online.

---

[26] SIMMEL G., *Über sociale Differenzierung, Leipzig*, Duncker & Humblot, 1890, p. 84.
[27] BAUMAN Z., *Modernità Liquida*, Laterza, 1999.
[28] PERFETTI S., PONZIANO R., *Le Trasformazioni dell'Intimità tra Dis-umanizzazione e Social Media – The Transformations of Intimacy between De-humanization and Social Media*, Media Education, Vol. 8, 2017, pp. 87.

Nel mondo odierno iperconnesso, le barriere tradizionali sono venute meno, lasciando emergere tra gli inediti modelli normativi di interazione sociale anche un nuovo tipo di intimità, l'intimità "*digitale*"[29]. A tal riguardo, il mutamento della configurazione dell'intimità individua una ri-personalizzazione delle relazioni interpersonali, che vengono fortemente supportate dai social media. In particolare, il tratto determinante della reciprocità di tali tecnologie riconfigura i caratteri sociali, favorendo gli scambi di contenuti personali[30] e, anche, la virtualizzazione di incontri e di rapporti affettivi che, in Italia, crea, forse, ancora, qualche imbarazzo.

Le *Dating App*, attualmente tipiche del mondo delle relazioni romantiche, inizialmente, erano nate come aiuti sociali, come accade per *Inclov*, applicazione indiana fondata nel 2016 da Kalyani Khona e Shankar Srinivasan, per creare un luogo inclusivo in cui persone con disabilità possono trovare il proprio coniuge e superare le inibizioni sociali e l'emarginazione derivante dalla disabilità.

L'app indiana nasceva da una precedente startup del 2014, denominata *Wanted Umbrella*, al fine di fornire servizi di *match-making*, attraverso questionari dettagliati e conseguenti calcoli di compatibilità, dedicati a soggetti affetti da disabilità, fornendo un modo per interagire con persone con interessi simili, concentrandosi sulla creazione di uno spazio sociale, organizzando eventi, studiati per favorire l'approccio interpersonale e superare lo stigma sociale nei confronti della disabilità.

Attualmente, in sostituzione del sistema di *match-making app*, sebbene non del tutto abbandonato, il modello predominante è rappresentato da diverse applicazioni, basate su profili pubblici "*double opt-in*", partendo dall'antesignana *Match.com*, per poi approdare ai diversificati *Tinder*[31], *Bumble, Grindr, Happn, OkCupid, Feeld,*

[29] SCARCELLI M., *Intimità Digitali. Adolescenti, amore e sessualità ai tempi di internet*, ed. Franco Angeli, 2015.
[30] CHAMBERS D, *Social Media and Personal Relationshisp. Online Intimacies and Networked Friendship*, Basingstoke, Palgrave Macmillan UK, 2013, pp. 61-81.
[31] *Tinder* è la principale app per smartphone di appuntamenti online, basata su immagini, con la quale gli utenti vengono presentati a potenziali partner, filtrati dalle preferenze in termini di orientamento sessuale, età e prossimità geografica. I potenziali partner vengono generalmente presentati con alcune fotografie, una breve introduzione biografica, informazioni su età, stato di istruzione/lavoro. L'app è stata fondata nel 2012 in Hatch Labs, gestito da *InterActiveCorp* (ex società madre di *Match Group*). Dopo essere stato inizialmente testato in una serie di campus universitari statunitensi, Tinder ha elaborato 350 milioni di "*accessi per scorrimento" (swipe right*) al giorno entro il 2013, salendo a un miliardo prima della fine del 2014. Anche con la concorrenza di *Bumble* negli Usa e di *Badoo* in Europa e di altre applicazioni similari, tuttavia, Tinder rimane l'app di appuntamenti più popolare, con 75 milioni di utenti attivi mensili e di 6,2 milioni di abbonamenti mensili. (IQBAL M. *Tinder Revenue and Usage Statistics*, 2018. Business of Apps, 27.02.2017.

eHarmony, The League, Tantan (Cina), Badoo, che consentono di creare istantaneamente un'interazione sociale, attraverso la segnalazione del soggetto online, trasformando definitivamente il mondo delle relazioni interpersonali.

Non mancano, tuttavia, esempi stravaganti di servizi di incontri basati su criteri scientifici, come *ScientificMatch.com* o *GenePartner.com* che promettono relazioni durature sulla base di informazioni genetiche e abbinano i soggetti in base alle differenze tra i loro sistemi immunitari.

Questo singolare approccio si fonda su di uno studio condotto da Claus Wedekind dell'Università svizzera di Berna che ha chiesto alle volontarie di annusare le magliette indossate da uomini, per tre giorni consecutivi e di classificarle in base all'attrattiva provata.

Lo studio ha rilevato che la maggior parte delle donne era attratta da uomini il cui sistema immunitario differiva maggiormente dal proprio. Ciò che spiegava le differenze del sistema immunitario a livello genetico erano le sequenze nei geni che codificavano l'antigene leucocitario umano (HLA)[32].

Per Eva Illuz, sociologa e antropologa all'Università ebraica di Gerusalemme, siti web come i suddetti ScientificMatch.com o Gene Partner.com includerebbero, quindi, un fattore "*fisico*", facendo dell'informazione genetica il punto di partenza per trovare un'affinità e/o una corrispondenza, sottolineando che, sebbene le piattaforme online debbano offrire agli utenti la possibilità di evidenziare la propria "*unicità*", la loro autorappresentazione, tuttavia, segue spesse canoni consolidati di conformità, standardizzazione e replicabilità. Al contrario, le informazioni genetiche sulla compatibilità biologica non sono standardizzate e rappresentano davvero l'unicità dell'individuo[33].

2. Condotte di *Catfishing, Grooming, Romance Scam, SexTortion, Teen Dating Violence.* Rilievi di diritto penale ed analisi giurisprudenziale

Il *Digital Dating*, sebbene affondi le proprie radici in modelli sociologici della prima era di Internet, l'attuale contesto rivela una pratica sociale generalizzata, utilizzata non solo per incontri occasionali ma anche per instaurare vere e proprie relazioni. Considerata la forte attrattività dei suddetti servizi, i rischi derivanti dall'utilizzo di

[3232] WEDEKIND C., SEEBECK T, BETTENS F., PAEPKE AJ (1995) *MHC-dependent mate preferences in humans.* Proc. Biol. Sci. 260, pp. 245-249.
[33] ILLOUZ E. *Cold Intimacies. The Making of Emotional Capitalism*. Cambridge, UK, 2007.

queste applicazioni, tra l'altro in materia di privacy, vengono spesso trascurati, in nome del reputato superiore ed assorbente interesse ad un incontro sentimentale.

Le applicazioni di incontri, invero, richiedono l'inserimento di molteplici dati sensibili, cioè "*altamente personali*", come preferenze sessuali e la posizione geografica. Nello specifico, la costruzione di un profilo all'interno di una piattaforma di *digital dating*, a differenza di quanto accade nel mondo analogico *off-line*, comporta la necessaria rivelazione di dettagli numerosi, anche molto personali, come i tratti della personalità o convinzioni religiose o politiche, in quanto forte è la pressione psicologica di costruire una dettagliata e convincente rappresentazione di sé[34].

L'evoluzione tecnologica ha, infatti, permesso la creazione di ambienti virtuali personalizzati dove gli utenti costruiscono realistiche ma non reali rappresentazioni identitarie e, dunque, la frammentazione e moltiplicazione infinita di identità, creando ancora una volta un'identità liquida (v. supra). Data la varietà dei *social network* a disposizione, non è difficile che il medesimo soggetto crei e diffonda diverse immagini di sé, delle "*maschere*", anche molto discordanti tra loro[35], attraverso il cambiamento di genere (*gender-swapping* o *gender-switching*), mutamento di razza, falsificazione dell'età anagrafica, fino all'utilizzo di immagini altrui, ricorrendo a vere e proprie manipolazioni.

In tale contesto si è così diffuso il fenomeno noto come *Catfish*, termine che gergalmente individua "*quel soggetto che si finge qualcun altro per intraprendere una relazione con un soggetto conosciuto online e che agisce, dunque, come un'esca che trae in inganno la vittima*"[36].

Nel caso del *Catfishing*, chi agisce, dapprima, costruisce un'identità non corrispondente alla propria utilizzando un profilo falso, immaginario o frutto della sottrazione di dati personali appartenenti ad altri soggetti e successivamente, dopo aver individuato la "*vittima*" e dopo averla contattata, cerca di acquistarne la fiducia e la confidenza.

---

[34] TOMA C.L., HANCOCK J.T., *Looks and Lies: Self-presentation in Online Dating Profiles*, Communication Research, 2010, n. 37, pp. 335-351.
[35] LORUSSO P., *L'insicurezza dell'era digitale, tra cybercrimes e nuove frontiere dell'investigazione*, Ed. Franco Angeli, 2011, p. 77.
[36] *Catfish: The TV Show*, è una serie televisiva-reality americana in onda su MTV, che racconta verità e bugie delle relazioni online. La serie è basata sul docufilm Catfish, prodotto nel 2010. L'idea della serie deriva dall'esperienza di Nev Schulman, conduttore della serie, che scoprì che la donna con cui aveva una relazione online non era stata onesta nel descriversi (FACCIOLI M., *Cyberbullismo ovvero il bullismo ai tempi del web: Analisi e riflessioni su un sopruso sempre al passo coi tempi*, Ed. Key, 2017, p. 90).

Nonostante possa sembrare, *prima facie,* una condotta del tutto innocua, in realtà, finisce per ledere la vittima nella sua sfera più intima, provocandone danni emotivi, danneggiandone la reputazione sociale, tanto nell'ambiente di lavoro quanto nelle relazioni sociali.

Le ragioni di tali condotte sono oscure quanto complesse, ma possono essere radicate nell' "*effetto disinibizione online*", in cui il potenziale di anonimato negli spazi online riduce la reattività delle persone ai codici sociali e morali. C'è un certo piacere nell'inganno, nel sapere di essere riusciti a ingannare qualcuno in qualche modo[37]. Attesa la natura di tali condotte, la giurisprudenza ha riconosciuto l'applicabilità ai casi di specie del reato di sostituzione di persona ex art. 494 c.p., definito come "*caposaldo della tutela penale dell'identità digitale"*[38].

Si è, infatti, ritenuto che "*integra il delitto di sostituzione di persona (art. 494 cod. pen.) la condotta di colui che crea ed utilizza un "profilo" su social network, utilizzando abusivamente l'immagine di una persona del tutto inconsapevole, associata ad un "nickname" di fantasia ed a caratteristiche personali negative" (cfr. Cass., Sez. 5, Sentenza n. 25 774 del 23/04/2014); ed ancora "integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale*"[39]

La natura chiaramente plurioffensiva del reato de quo è stata pacificamente riconosciuta dalla Suprema Corte secondo cui "*oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p. è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che*

[37] D. COSTA K., *Catfishing: the truth about deception online,* in https://blogs.scientificamerican.com/anthropology-in-practice/catfishing-the-truth-about-deception-online/, 2014.
[38] CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14.08.2013 n. 93, conv. Con modificazioni dalla l. 15.10.2013 n. 119*, in *Cassazione penale*, 2014, n. 3, pp. 1094-1105.
[39] Cfr. Cass., V Sez., 08 novembre 2007, n. 46674; Tribunale di Pescara, 12 febbraio 2021, n. 2246.

possono superare la ristretta cerchia di un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome"[40].

Il pregio della suddetta pronuncia consisteva nell'aver esteso l'applicabilità del delitto ex art. 494 c.p. anche se commesso in rete, trattandosi, nel caso esaminato dagli Ermellini, di un soggetto che aveva creato ed utilizzato un account di posta elettronica, attribuendosi falsamente generalità altrui, inducendo in errore gli utenti della rete nei confronti de quali le false generalità erano state declinate, agendo con l'esclusivo fine di arrecare danno al soggetto le cui generalità erano state spese senza il suo consenso.

I giudici di legittimità hanno, indi, chiarito che il delitto di sostituzione di persona può realizzarsi sia mediante la sostituzione fisica di una persona ad un'altra, sia attraverso la falsa attribuzione di nome, stato o qualità e in questo caso la manifestazione esteriore della condotta può avvenire in qualunque modo.

Alteris verbis, il reato non si è consumato nel momento in cui si è creato l'account di posta elettronica, ma nel momento in cui sono stati indotti in errore gli utenti che, ritenendo di interloquire un una determinata persona, in realtà, inconsapevolmente si sono trovati ad avere a che fare con persona differente.

Le falsità personali, infatti, sono caratterizzate dal contenuto della rappresentazione e non dalla forma, tanto che si è ritenuto di tutelare la corrispondenza ai fatti di alcune dichiarazioni o enunciati assertivi che, qualunque forma abbiano, si riferiscono ad oggetti di identificazione o qualificazione personale che determinano un'aspettativa sociale di corrispondenza ai fatti di tutte le forme di rappresentazione che li riguardano. E, dunque, oggetto materiale del reato di falsità personale non è tanto la "*fisicità*" della persona, quanto il complesso delle caratteristiche, degli attributi, delle qualità, che fanno sì che una persona si distingua dalle altre, per gli effetti ad essi caratteristici attribuiti dalla legge.

A tale oggetto, fa da contraltare l'obbligo giuridico del cittadino di farsi conoscere quello che è, in determinate situazioni giuridiche e in particolari rapporti. Occorre, dunque, chiedersi se, e in che misura, possa sorgere tale obbligo in internet e quali siano le aspettative che gli utenti ripongono circa la veridicità delle identità con cui entrano in relazione.

[40] Cfr. Cass. Pen. Sez. V, 14 dicembre 2007, n. 46674.

Appare, così, evidente che, nelle relazioni che si svolgono su internet, l'esigenza di tutela della fede pubblica si fonda sul fatto che l'utente possa rappresentarsi l'identità digitale come corrispondente ad una persona fisica, con la conseguente possibilità di trasferire detta relazione nel mondo reale.

A questo punto si potrà verificare la riconducibilità del caso concreto alla fattispecie astratta, valutando il verificarsi dell'evento (l'induzione in errore dell'utente), la condotta tenuta (l'attribuzione di falso nome, stato, qualità) e la sua idoneità (considerando anche se il contesto nel quale si svolge la vicenda può creare affidamento nell'utente), la presenza del dolo specifico in capo all'agente (intenzione di ingannare a fine di vantaggio o di danno)[41].

Trasponendo tali argomenti ai servizi di social network, è evidente come la richiamata disciplina ricomprenda, altresì, le condotte di coloro che *"creano un profilo su un social network, utilizzando abusivamente la foto di un altro soggetto del tutto inconsapevole, al fine di comunicare a mezzo chat con gli altri utenti inducendoli in errore*"[42].

Il caso della sostituzione di persona, attraverso l'uso perverso della tecnologia online, è stato affrontato a più riprese anche recentemente dalla Suprema Corte[43] che ha ribadito il principio secondo il quale "*integra il delitto di cui all'art. 494 c.p. la condotta di colui che crea ed utilizza abusivamente l'immagine di un altro soggetto, inconsapevole, per creare un profilo su social network con identità digitale non corrispondente a colui che, di fatto, lo utilizza*"[44].

Il *Digital Dating*, tuttavia, presenta ancora tante insidie, ancora una volta legate all'intento di palesare all'interlocutore delle piattaforme social e potenziale partner un'immagine migliore di sé, trasformandosi in una condotta suscettibile di realizzare azioni fraudolente. Di qui, le sempre più ricorrenti cd. Truffe romantiche o *Romantic Scam* o *Love Scam*, quali truffe online connotate dalla componente sentimentale, con

[41] FLICK C., *Falsa Identità su Internet e Tutela Penale della Fede Pubblica degli Utenti e della Persona*, Nota a Cass. Pen. 08.11.2007 n. 46674, Dir. Informatica, fasc. 4-5, 2008, p. 526.
[42] Cfr. Cass. Pen. Sez. V, 16.06.2014 n. 25774.
[43] Cfr. Cass. Pen. Sez. V, 06.07.2020 n. 22049.
[44] Cfr. Cass. Pen. Sez. V, 8 giugno 2018, n. 42572, in C.E.D. Cass., n. 274008; Sez. V, 23 aprile 2014, n. 25774, nella quale viene stabilito che integra il delitto di sostituzione di persona la condotta di colui che crea ed utilizza un profilo su *social network* impiegando abusivamente l'immagine di una persona del tutto inconsapevole, associata ad un nickname di fantasia nonché a caratteristiche personali negative. La descrizione di un profilo social poco lusinghiero evidenzia sia il fine di vantaggio, consistente nell'agevolazione delle comunicazioni e degli scambi di contenuti in rete, sia il fine di danno per il terzo, di cui è abusivamente utilizzata l'immagine. V. anche Sez. III, 15 dicembre 2011, n. 12479, ivi, n. 252227; Sez. V, 8 novembre 2007, n. 46674.

il tipico *modus operandi* di navigare in internet con un falso profilo e di contattare la propria vittima su di una piattaforma internet, scambiando, dapprima, messaggi e, indi, sempre più rapidamente, dichiarando il proprio amore e creando una dipendenza affettiva.

Per settimane o mesi la presunta relazione amorosa si sviluppa via Skype, Facebook o altre piattaforme ma, al momento di conoscersi personalmente, il truffatore (o truffatrice) asserisce di essere stato coinvolto in un incidente, di essersi ammalato, di essere stato derubato *et similia*, richiedendo, così, alla vittima, ormai illusa ed innamorata, di sostenere i costi del viaggio, delle spese sanitarie, senza considerare che l'agognato incontro giammai si avvererà.

Il successo delle truffe relazionali o *Romance Fraud* sembra dovuto alla loro duplice natura; da un lato viene, infatti, alimentata la motivazione a instaurare una relazione romantica e, di conseguenza, a creare fiducia tra la vittima e il truffatore, dall'altro viene indotta la volontà di trasferire denaro al partner virtuale.

Un caso recente sul tema, affrontato dalla giurisprudenza di merito[45], ha descritto il tipico esempio della truffa sentimentale ai danni del malcapitato che riferiva di aver intrapreso un'amicizia virtuale con una donna conosciuta a mezzo Facebook, dal 2018 al 2019, e di aver iniziato a scambiare alcuni messaggi sul servizio di messaggistica Messenger con la suddetta la quale, tuttavia, aveva posto in essere una serie di artifizi al fine di procurarsi un ingiusto profitto.

La donna aveva iniziato a carpire la fiducia dello sventurato e la sua amicizia, inviando messaggi lusinghieri ed instillando nello stesso un forte senso di pietà, raccontando di lavorare in Germania come badante presso una famiglia presso la quale subiva angherie, di non essere remunerata congruamente, di patire di problemi di salute e di non avere familiari o amici che potessero aiutarla.

La relazione virtuale veniva portata avanti ogni giorno, diventando progressivamente sempre più intima tanto che la stessa persona offesa si confidava con la predetta che, con il suo atteggiamento, aveva convinto che l'amicizia virtuale potesse trasformarsi in una storia d'amore vera e propria.

Dopo un improvviso – e strategico – periodo di silenzio, la donna raccontava di aver urgente bisogno di soldi, convincendo il suo consueto interlocutore ad inviare, inizialmente, piccole somme di denaro su di una scheda prepagata, di cui ignorava

[45] Cfr. Tribunale Catania, sez. I, 11 gennaio 2021, n.reg. 3562/2020.

l'intestatario, per poi versare somme più consistenti, corrispondenti a circa euro 200/300/500 versati quotidianamente. A questo punto della relazione, come si ricava dalla deposizione della persona offesa, la donna raccontava di essere riuscita a fuggire dalla Germania e di essere riuscita ad approdare a Roma, ove, sfortunatamente, aveva subito una rapina, chiedendo, nuovamente, ma stavolta in maniera più pressante, altre più consistenti somme di denaro di circa euro 4.000,00. Di qui il tribunale catanese ha riconosciuto la prassi della *romantic scam,* come posta in essere da persone che adescano altri soggetti "*deboli*", tramite i social network, creando veri e propri profili attraenti e spesso generando false identità online, scambiando con le vittime designate lunghi messaggi lusinghieri per alcuni mesi allo scopo di creare un rapporto di apparente fiducia con l'obiettivo finale di truffare le vittime in cambio di denaro con la scusa di superare temporanee difficoltà finanziarie.

Nella "*truffa romantica*", l'elemento *"truffa*", rilevante ex art. 640 c.p.c, non si apprezza tanto per l'inganno in sé riguardante i sentimenti dell'agente rispetto a quelli della vittima, ma perché la menzogna circa i propri sentimenti è intonata con tutta una situazione atta a far scambiare il falso con il vero operando sulla psiche del soggetto passivo.

A tal proposito, va chiarito che, per ricostruire l'elemento oggettivo del reato, si deve tener presente la concatenazione delle note modali della condotta truffaldina e dei conseguenti eventi, nella sequenza indicata dal Legislatore artifizi o raggiri – induzione in errore – atto dispositivo – danno patrimoniale e profitto ingiusto, sottolineando in particolare che, ai fini della individuazione della condotta truffaldina, occorre accertare l'idoneità ingannatoria degli artifizi o raggiri e il nesso causale tra l'inganno e l'errore della vittima la quale, incisa nella sua sfera volitiva da falsi motivi, si determina ad una certa scelta patrimoniale che altrimenti non avrebbe effettuato; dovendosi, invero, valorizzare ai fini della valutazione del delitto in esame la illiceità di comportamenti che, sfruttando la situazione di debolezza della vittima, nella specie coinvolta in una relazione sentimentale a distanza, hanno dato luogo a falsi motivi, determinanti la scelta patrimoniale del disponente.

Ed infatti, gli artifici, intesi come manipolazione esterna della realtà provocata mediante la simulazione di circostanze inesistenti o, per contro, mediante la dissimulazione di circostanze esistenti – o il raggiro consistente in un'attività simulatrice, sostenuta da parole o argomentazioni atte a far scambiare il falso con il vero, sono en-

trambi mezzi per creare un erroneo convincimento, passando il primo attraverso il camuffamento della realtà esterna e operando il secondo direttamente sulla psiche del soggetto"[46].

All'interno delle relazioni sentimentali, anche e soprattutto digitali, con peculiare attenzione agli adolescenti, si è focalizzata l'attenzione sulle dinamiche di prevaricazione attraverso le nuove tecnologie, potendosi parlare di *Teen Dating Violence* e di *Cyber Dating Abuse*, ogni qualvolta venga messo in atto un qualsiasi comportamento che pregiudichi lo sviluppo o la salute del partner, compromettendone la sua integrità fisica e psicologica, e anche di *Sex-Tortion*, quali casi di estorsione e di coercizione sessuale online[47].

In tal senso, infatti, si individuano tutte quelle condotte estorsive in cui i contenuti multimediali sessualmente espliciti vengono utilizzati per estorcere alla vittima favori sessuali e/o denaro, dietro minaccia della loro diffusione online.

Vi possono essere diverse tipologie tra le quali si registrano le condotte estorsive, individuando una prima in cui le immagini possono essere il frutto di un'attività di *hacking*, cioè di accesso non autorizzato al sistema informatico in uso alla vittima: vengono prelevati dal computer o da altri dispositivi o servizi di cloud storage immagini o video intimi o sessualmente espliciti prodotti consensualmente e per fini propri[48].

Non vi è alcun contatto precedente con la vittima, la quale viene contattata solo una volta andato a buon fine l'accesso non consentito e, a tal punto, viene ricattata con la richiesta di pagamento solitamente in bitcoin o in altra moneta virtuale per poter accedere nuovamente ai propri contenuti o per ricevere via e-mail un programma per la decriptazione.

Può, altresì, accadere che le condotte di *sextortion* si sviluppino secondo un processo più lungo che coinvolge maggiormente la vittima, sempre avvalendosi di ambienti virtuali, come chat o, per lo più, di servizi di *online dating*, inteso come bacino di potenziali utenti vulnerabili, che vengono attirati, utilizzando un profilo falso, creato ad hoc, come nel caso succitato delle *romance fraud*.

---

[46] Cfr. Cass. Pen. N. 25165/2019; sez. II, n. 42941/2014; sez. II, n. 42867 del 20.06.2017; sez. V, n. 11441/1999; sez. I, n. 16264/1990.
[47] WOLAK J., FINKELHOR D., *Sextortion: Findings from a Survey of 1.631 Victims*, www.unh.edu/ccr/pdf/Sextortion_RPT_FNL_rev0803.pdf, 2016.
[48] NICOLA H., POWELL A., *Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law*, in Social & Legal Studies, 2016, n. 25, pp. 397-418.

Una volta instaurato il contatto, la vittima viene adescata e lusingata e, poi, indotta a scambiare informazioni sempre più riservate ed intime, che saranno oggetto della futura condotta estorsiva.

A tal punto, interviene la consueta richiesta economica da parte dell'*offender*, dietro minaccia di una pubblica diffusione online dei materiali intimi fino ad allora condivisi, con un significativo impatto sia psicologico sia reputazionale. Spinte da un profondo senso di vergogna e disagio, le vittime tendono ad assecondare l'*offender* e a non denunciare il fatto. O ancora, si rammenti il *Grooming*, espressione con cui si identifica l'adescamento in rete a scopo sessuale basato sul plagio psicologico.

Il *Grooming* è una forma di abuso sessuale online in cui l'elemento centrale è, anche in questo caso, la costruzione graduale di un "*legame affettivo tecnomediato*" tra adulti e solitamente minori[49]. La relazione affettiva e di fiducia che si instaura diventa per l'adulto il pretesto per inviare sollecitazioni sessuali al minore e avviare uno scambio di contenuti sessualmente espliciti. Allorquando il minore si rifiuti di proseguire la "*relazione*", intervengono minacce di diffusione dei contenuti scambiati[50]. Posto che il fenomeno, ancora fortemente sommerso e sottodimensionato, ha i suoi preminenti aspetti sociologici, non si rinvengono casi giurisprudenziali in quanto l'ordinamento non conosce alcuna definizione di *Sextortion.*

A fronte di siffatte condotte, possono, dunque, trovare applicazioni diversi fattispecie e, *in primis*, la già analizzata ipotesi di sostituzione di persona ex art. 494 c.p.

Emerge, in ogni caso, il reato di estorsione, previsto e punito all'art. 629 c.p., che punisce colui che *«mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno»*, atteso che tale fenomeno si estrinseca nel ricorso alla minaccia diretta, dapprima a determinare in capo alla vittima uno stato di costrizione psichica e, poi, a ottenere un profitto ingiusto per sé o altri con correlativo danno per la vittima. Attraverso la prospettazione di vedere pubblicate le proprie immagini intime *on line* viene, infatti, indotto nella vittima un timore tale da costringerla all'atto di disposizione patrimoniale

Per quanto concerne, *per contra*, la modalità attraverso cui il soggetto agente si procura il materiale sessualmente esplicito, violando illecitamente il dispositivo in uso alla vittima, troverà applicazione la disposizione ex art. 615-ter c.p., in materia di

[49] ALLEGRO, NANNI E PUGLIESE, 2012.
[50] SAVONARDO L. a cura di, *GenerAzioni Digitali, Teorie, pratiche e ricerche sull'universo giovanile*, ed. Egea, 2020, pp. 235-236.

accesso abusivo ad un sistema informatico o telematico, secondo cui «*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni*».

Viene in tal modo perseguita tanto la violazione delle misure di protezione quanto l'accesso abusivo dei settori di memoria protetti da parte di un soggetto non autorizzato.

Intervenendo poi sui dati informatici altrui, può dirsi applicabile anche la fattispecie prevista all'art. 635-bis c.p. in materia di danneggiamento di informazioni, dati e programmi informatici.

3. Il Dating Digitale e la tutela della privacy. I suggerimenti del Garante Privacy.

Non da ultimo, unitamente ai profili rilevanti da un punto di vista penale, occorre valutare se il settore dell'*online dating* sia compatibile con il diritto alla privacy, data l'immissione di immagini e la condivisione di informazioni riservate e personalissime. Tutte le app di incontri richiedono, infatti, la diffusione di informazioni personali da parte degli utenti stessi, con l'intenzione di abbinarle alle preferenze espresse. Molti utenti, ad esempio, ignorano che l'immissione di nome, foto, indirizzi mail, possano essere combinati o aggregati con altri dati come la geolocalizzazione (richiesta obbligatoriamente in talune app come *Tinder, Bumble, Happn ed Her*) o la cronologia di consultazione di siti. Tali dati sono dettagli di cui gli utenti potrebbero non essere a conoscenza e vengono raccolti, archiviati e condivisi al di fuori del contesto delle applicazioni di appuntamenti. Si citi l'esempio di *Grindr*, un'applicazione di incontri LGBTQ, che consente di condividere, anche, la data più recente del test HIV[51].

[51] La notizia che l'app stava condividendo i dati relativi allo stato HIV degli utenti, inclusa la data dell'ultimo test, attraverso le società Apptimize e Localytics, era apparsa su di un articolo di BuzzFeed del 03.04.2018 per il quale "*Because the HIV information is sent together with users' GPS data, phone ID, and email, it could identify specific users and their HIV status, according to Antoine Pultier, a researcher at the Norwegian nonprofit SINTEF, which first identified the issue*." (*Grindr in letting other Companies See User IIV Status and Location Data*). Lo stesso Grindr si difendeva assumendo che la possibilità conferita agli utenti di pubblicare informazioni anche relative allo stato HIV veniva già chiarito nella politica sulla privacy al momento dell'iscrizione, pur specificando che le informazioni in parola non sarebbero mai state vendute a terzi o a inserzionisti. *Grindr*, tuttavia, ha successivamente modificato la propria policy, cessando di fornire le suddette informazioni ai fornitori Apptimized e Localytics "*As the testing of our feature has completed, any information related to HIV status has been removed from Apptimized and we are in the process of discussing removal of this data from Localytics."* (cfr. il sito: *https://www.npr.org/sections/thetwo-way/2018/04/03/599069424/grindr-admits-it-shared-hiv-status-of-users?t=1654415534122*).

A tale ultimo proposito, per l'app *Grindr* la Norvegia, nel 2020, ha aperto una procedura di infrazione dopo aver raccolto diverse segnalazioni e reclami nonchè una relazione da parte di un'associazione di consumatori (Beuc) che sostenevano l'illecita profilazione online da parte dell'app di incontro LGBTQ finalizzata ad annunci di marketing mirati in base ai gusti sessuali degli utenti *Grindr*, senza alcuna prestazione di consenso da parte dell'interessato.

Il tutto in palese contrasto con l'art. 4 del GDPR che richiede che il consenso debba consistere in *"una manifestazione libera, specifica, informata ed inequivocabile".*

Tra l'altro, anche in base al Considerando 32, "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".*

La condivisione eccessiva delle informazioni personali nelle app di appuntamenti o persino nei social media può condurre, altresì, alla raccolta e all'utilizzo dei dati medesimi da parte di un *doxer*. Per *Doxing*[52] si intende la pratica di ricerca, condivisione e pubblicizzazione delle informazioni personali degli utenti sul web attraverso un sito, un forum o un profilo social. Il tutto senza che il soggetto abbia acconsentito alla diffusione delle sue informazioni più riservate sulla Rete. Alcuni dati sono legalmente disponibili, attraverso profili social, database pubblici, altri, invece, possono essere recuperati in maniera illecita attraverso pratiche di hacking o dal *Dark*

[52] "*Doxing is the intentional public release onto the internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual*". DOUGLAS D.M., *Doxing: a conceptual analysis*, in Ethics and Information. Technology, vol. 18, settembre 2016, pp. 199-2010.

Web. Oltre alle informazioni personali, il *Doxing* è sovente usato per rendere pubblici indirizzi e-mail, orientamenti politici, foto compromettenti di un individuo, soprattutto se trattasi di personaggi pubblici.

Sebbene tali informazioni, come indirizzi e-mail, immagini siano già online, con la pratica del *Doxing*, queste informazioni vengono traslate da diversi fonti in un unico ambiente digitale, rendendole disponibili e accessibili a chiunque. Proprio perché si tratta di informazioni già diffuse, la pratica del *Doxing* non viene considerata alla stregua di una pratica illecita, sebbene la maggior parte dei servizi online e delle piattaforme, sempre più frequentemente, abbiano adottato politiche *antidoxing*[53], restando, comunque, sempre consigliabile usare VPN e nascondere le informazioni sulle registrazioni dei domini su WHOIS.

Anche e soprattutto nel settore del *dating* digitale, quindi, i dati immessi sono suscettibili di compromissione. In Giappone, l'applicazione autoctona di appuntamenti, *Omiai*, aveva raccolto 1,71 milioni di dati personali immessi dagli utenti, inclusi foto ed indirizzi, atteso che la peculiarità dell'applicazione di dating giapponese è rappresentata dall'obbligo di inserire la copia di un documento valido (patente, documento di identità e anche copia dell'ultimo titolo di studio conseguito) per ottenere l'apertura di un account, ciò al fine di trovare una combinazione migliore ed un'affinità maggiore con la persona interessata ad instaurare una relazione. Molte identità virtuali sono state compromesse anche con l'app *Ashley Madison*, piattaforma canadese assai celebre per incontri extraconiugali, che nel 2015 ha registrato oltre 60 gibabyte di dati personali fuoriusciti dai database aziendali. Un altro caso di esposizione dannosa dei dati immessi online è rappresentato dalla community di *Escort Reviews* e dal sito web *Meetmindful.com*, violati da hacker che avevano pubblicato l'intero database del sito di accompagnatrici e di incontri, comprensivo di nomi, indirizzi, date di nascita, dettagli fisici, indirizzi IP, geolocalizzazioni e credenziali per accedere ai social network, con il rischio di pervenire all'identificazione e localizzazione degli utenti, esposti alla già descritta pratica di ricatti e di *sextortion*.

Le minacce alla *privacy* che gli utenti devono affrontare sono, dunque, costanti, come ha rivelato una ricerca di Kaspersky, secondo cui il 40% di soggetti intervistati ha ammesso che, durante le interazioni online, il proprio partner ha condiviso schermate della conversazione in essere, in assenza di consenso, minacciato di divulgare

[53] Cfr. https://www.privacyitalia.eu/pericoli-internet-cose-doxing-difendersi/4565/, 17.10.2017.

informazioni personali rese, diffuso foto intime e perseguitato nella vita offline, il che è anche una diretta conseguenza del fenomeno del *Doxing*.

Anna Larkina, esperta di sicurezza di Kasperky si è così espressa "*in effetti, i social media e varie app hanno reso gli appuntamenti molto più facili per noi. l'amore della tua vita online, ma sfortunatamente ci sono anche bot e truffatori che cercano prede su piattaforme di trovare incontri. Ecco perché mentre si comunica con qualcuno online, è comunque importante ricordare le regole di base della privacy digitale. Per uscire con qualcuno online in modo sicuro, ti consiglio di non condividere le informazioni di identificazione personale, come il tuo numero di telefono, posizione, casa e indirizzo di lavoro, ecc. Prevenire le minacce in una fase così precoce ti aumenterà di goderti gli appuntamenti online senza alcun timore*"[54].

Al fine di stimolare la consapevolezza circa l'utilizzo di siti e di app di dating digitale, a fronte dei rischi più o meno imponenti per la privacy, data la fallacia dei sistemi di crittografia e dei protocolli di protezione nei siti in discorso, il Garante per la Protezione dei Dati Personali ha pubblicato un decalogo di suggerimenti e di cautele per gli utenti dei siti di dating.

L'attenzione da profondere nell'utilizzo dei programmi ormai di uso comune tra i più giovani e meno giovani si articola, infatti, su più fronti, tutti affrontati dal Garante, sebbene l'utilizzo di una dating app su una rete pubblica WIFI non protetta, già espone al rischio che una foto inviata o un'informazione personale immessa in rete possa essere sottratta da un hacker, nemmeno troppo esperto, che potrebbe adoperarla per attuare una condotta lesiva. A ciò aggiungasi il rischio di *malware*, molto più elevato su sistemi Android rispetto a iOS.

La scheda elaborata dal Garante, lungi dallo scoraggiare o distogliere dall'uso di tali applicazioni, invita, tuttavia, ad assumere taluni accorgimenti e cautele nell'utilizzo delle dating app, invitando a:

- leggere sempre con attenzione l'informativa sul trattamento dei dati personali, onde comprendere quali dati verranno raccolti e per quanto tempo verranno

[54] "*Indeed, social media and various apps have made dating much easier for us. You might find the love of your life online but unfortunately, there are also bots and fraudsters looking for prey on dating platforms. That is why while communicating with someone online, it is still important to remember the basic rules of digital privacy. To date online safely, I recommend not sharing personal identifying information, such as your phone number, location, home, and work address, etc. Preventing threats at such an early stage will let you enjoy online dating without any fears*", in Privacy Risks of Online Dating: Every 6th user has been doxed while looking for a relationship, 19.07.2021.

conservati e se potranno essere condivisi e/o ceduti a terzi per finalità commerciali o altro;

- fornire solo i dati indispensabili, disattivando gli strumenti di raccolta di informazioni non essenziali, limitando le possibilità di accesso da parte delle app ad altre funzionalità presenti sullo smartphone (microfono, camera) e disattivando l'accesso ai dati tramite geolocalizzazione, che in maniera occulta possono costituire violazione della privacy;
- utilizzare preferibilmente un nickname o uno pseudonimo, evitando di adoperare, al momento dell'iscrizione, la propria mail ufficiale o abituale che non contenga riferimenti al nome e cognome;
- riflettere se essere riconoscibili attraverso la pubblicazione di una foto profilo o di caricare video personali o di condividerle in privato, al fine di evitare di cadere vittima di fenomeni di sextortion, di revenge porn o di deep nude. Si consideri, inoltre, che i dati biometrici del volto sono attualmente utilizzati come password per smartphone.
- Evitare di memorizzare su siti o app di dating dati come coordinate di accesso a carte di crediti e a circuiti di pagamento;
- evitare di fornire a sconosciuti informazioni troppo personali, al fine di evitare condotte pericolose di *Catfishing*, di simulazione di falsa identità finalizzata a raccogliere informazioni utili per realizzare truffe ed altre condotte delittuose.
- premurarsi di cancellare periodicamente i dati raccolti dall'app di dating e, nel caso di cancellazione del servizio di dating, disattivare l'account personale ed eliminare tutti i dati ad esso collegati;
- impostare password di accesso complesse ed aggiornarle periodicamente alle nuove versioni delle applicazioni;
- evitare che i minori utilizzino siti per il dating, in quanto maggiormente esposti al rischio di diffusione, anche inconsapevole, di dati sensibili ed impostare limitazioni di uso sui dispositivi ai minori, sebbene il codice privacy stabilisce che solo a partire dagli anni 14 un minore può esprimere autonomamente il consenso al trattamento dei propri dati personali[55].

[55] GDPR, *Dating Online e Protezione dei Dati, Quando insegui Cupido Online, Fai Attenzione alla Privacy*!, in *https://www.gpdp.it/temi/internet-e-nuove-tecnologie/dating-online*.

LA DIGITALIZZAZIONE DELLE SENTENZE NEL PROCESSO

Di Gianluca Melillo

SOMMARIO. 1. Le peculiarità delle sentenze digitali tra processo telematico civile, tributario ed amministrativo. - 2.1. Le sentenze digitali nel processo civile. - 2.2. I provvedimenti emessi dalla Corte di Cassazione e dal Giudice di Pace. - 3. Le sentenze digitali nel processo tributario. - 4. Le sentenze digitali nel processo amministrativo. – 5. Note bibliografiche.

Abstract: *L'esigenza della digitalizzazione, avvertita da tempo nel comparto giustizia, investe i differenti settori del diritto processuale ed anche i provvedimenti dei Giudici, in maniera non uniforme.*

1. Le peculiarità delle sentenze digitali tra processo telematico civile, tributario ed amministrativo.

La diversa evoluzione e le diverse tempistiche con cui sono stati predisposti i procedimenti telematici innanzi alle autorità civili, tributarie ed amministrative[56] hanno comportato una differenziazione nelle specifiche tecniche che disciplinano i relativi processi (PCT, PTT e PAT[57]), che si ripercuotono inevitabilmente anche nell'ambito delle sentenze, relativamente alle modalità operative di emissione, estrazione di copia digitale ed alla conseguente notificazione.

[56] Per quanto le recenti vicende pandemiche hanno impresso un'accelerazione alla digitalizzazione - a fronte di una norma primaria risalente al 2009 - l'informatica applicata al processo penale è rimasta fortemente arretrata rispetto alle altre giurisdizioni e, per tale ragione, non può essere oggetto del presente approfondimento in difetto di un'apposita disciplina concernente la digitalizzazione dei relativi provvedimenti (Sul punto, cfr. JUSTICE-ER - *Percorsi e strumenti per una giustizia digitale al servizio del cittadino* – a cura di D. PIANA - Fondazione CRUI 2021).
Infatti, solo con l'art. 83, comma 12 *quater*, D.L. del 17 marzo 2020, n. 18, convertito con modificazioni nella legge del 24 aprile 2020, n. 27, ed ulteriormente modificato dal D.L. del 20 aprile 2020, n. 28, si è dato avvio al "Processo Penale Telematico". Più nello specifico, la prima fase, nata in periodo di emergenza sanitaria Covid-19, prevede il deposito con modalità telematica - attraverso il Portale dei Depositi atti Penali ospitato sul Portale dei Servizi Telematici - di memorie, documenti, richieste e istanze che possono essere "presentati dall'indagato" destinatario dell'avviso della conclusione delle indagini preliminari *ex* art. 415 *bis*, comma 3, c.p.p..
[57] Gli acronimi corrispondono rispettivamente a Processo Civile Telematico (PCT), Processo Tributario Telematico (PTT) e Processo Amministrativo Telematico (PAT); consequenzialmente, anche i relativi sistemi informatici differiscono: SICID per il civile, SIGIT per il tributario e SIGA per l'amministrativo.

Le peculiarità delle normative di riferimento sono dovute anche alla circostanza che le specifiche sono sostanzialmente riferibili a tre Ministeri differenti[58], ove – a fronte del processo telematico civile già rodato – non c'è stata la capacità e volontà di improntare su di questo le normative successive (amministrativa e tributaria).

Ciò può determinare una difficoltà pratica dell'operatore del diritto - nello specifico l'avvocato - che si trova a dover applicare procedure differenziate di volta in volta a seconda dell'Ufficio Giudiziario che emette il provvedimento di definizione del giudizio[59].

È quindi utile l'analisi delle diverse normative e modalità operative, al fine di individuare le principali differenze tra i tre procedimenti.

Le peculiarità sussistono sin dalla fase della redazione e deposito degli atti digitali per i magistrati, atteso che nel PCT l'art. 15, D.M. del 21 febbraio 2011, n. 44[60] non prevede un relativo obbligo per i giudici, essendo esplicitato che - ove un atto venga redatto in formato cartaceo - lo stesso debba essere convertito in formato digitale ed inserito nel fascicolo telematico. Per questioni tecniche (impostazione della consolle dei magistrati) l'unico atto che sicuramente verrà redatto come atto informatico è il decreto ingiuntivo.

L'art. 7, commi 1 e 2, D.P.C.M. del 16 febbraio 2016, n. 40[61] per il PAT, prevede invece che i provvedimenti del giudice siano redatti e depositati sotto forma

[58] Trattasi del Ministero della Giustizia per il civile, del Ministero dell'Economia e delle Finanze per il tributario e della Presidenza del Consiglio dei Ministri per l'amministrativo.

[59] Mentre un osservatore diverso dal giurista scorge nella digitalizzazione principalmente la leva per un incremento dell'efficienza e quindi per una migliore allocazione delle risorse (anche) economiche, oltre che per un potenziale risparmio dei tempi processuali, il teorico del diritto è chiamato a confrontarsi con le problematiche che il processo telematico pone. In ogni caso, la crescente informatizzazione dei professionisti ridonda in un allargamento della cultura digitale anche extra-giuridica e quindi potenzia *tout court* la c.d. cittadinanza digitale. Sul punto, v. JUSTICE-ER - *Percorsi e strumenti per una giustizia digitale al servizio del cittadino* – Fondazione CRUI 2021.

[60] Art. 15, D.M. 44/2011: "Deposito dell'atto del processo da parte dei soggetti abilitati interni. 1. L'atto del processo, redatto in formato elettronico da un soggetto abilitato interno e sottoscritto con firma digitale, è depositato telematicamente nel fascicolo informatico. 2. In caso di atto formato da organo collegiale l'originale del provvedimento è sottoscritto con firma digitale anche dal presidente. 3. Quando l'atto è redatto dal cancelliere o dal segretario dell'ufficio giudiziario questi vi appone la propria firma digitale e ne effettua il deposito nel fascicolo informatico.
4. Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia informatica nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34 e provvede a depositarlo nel fascicolo informatico, apponendovi la propria firma digitale".

[61] Art. 7, D.P.C.M. 40/2016. "Provvedimenti del giudice 1. I provvedimenti del giudice sono redatti e depositati sotto forma di documento informatico sottoscritto con firma digitale. I provvedimenti collegiali sono redatti dall'estensore, da questi sottoscritti e trasmessi telematicamente al presidente del collegio, che li sottoscrive e li trasmette telematicamente alla Segreteria per il deposito. 2. Il Segretario di

di documento informatico sottoscritto con firma digitale; quelli collegiali sono redatti dall'estensore, da questi sottoscritti e trasmessi telematicamente al presidente del collegio, che li sottoscrive e li trasmette telematicamente al segretario di sezione, che appone anch'egli la propria firma digitale e provvede al loro deposito nel fascicolo informatico.

Infine gli artt. 15 e 16, D.M. del 23 dicembre 2013, n. 163[62] per il PTT, prevedono le modalità per redigere il verbale ed i provvedimenti in via informatica, con sottoscrizione digitale. Per i verbali è espressamente previsto che, ove non si possa procedere in tal modo, verrà redatto verbale cartaceo, poi scansionato ed inserito nel fascicolo telematico. Nessuna norma prevede, comunque un obbligo preciso di redazione degli atti in originale informatico.

Difatti, a seguito della pubblicazione nella Gazzetta Ufficiale in data 13 novembre 2020, del Decreto del Direttore Generale delle Finanze che disciplina le regole tecniche-operative previsto dall'art. 3, comma 3, D.M. 163/2013, è data la "*possibilità*" ai giudici tributari di redigere il provvedimento giurisdizionale digitale (con decorrenza dal 1° giugno 2021 per tutte le Commissioni Tributarie)[63].

---

sezione sottoscrive con la propria firma digitale i provvedimenti di cui al comma 1, provvede al loro deposito nel fascicolo informatico e alla contestuale pubblicazione, mediante inserimento, nel SIGA e sul sito internet della giustizia amministrativa, con le cautele previste dalla normativa in materia di tutela dei dati personali, ed in particolare nel rispetto della disciplina dettata dagli articoli 51 e 52 del Codice dei dati personali, secondo le modalità stabilite dalle specifiche tecniche di cui all'articolo 19. 3. Il deposito del documento redatto su supporto cartaceo e sottoscritto con firma autografa è consentito esclusivamente quando il Responsabile del SIGA attesta che il sistema informatico non è in grado di ricevere il deposito telematico degli atti. In tal caso, il Segretario di sezione provvede ad estrarre copia informatica, anche per immagine, dei provvedimenti depositati, nei formati stabiliti dalle specifiche tecniche di cui all'articolo 19 e la inserisce nel fascicolo informatico. 4. Il deposito dei provvedimenti con modalità informatiche sostituisce, ad ogni effetto, il deposito con modalità cartacee".

[62] Art. 15, D.M. 163/2013: "Processo verbale dell'udienza 1. Il processo verbale dell'udienza, redatto come documento informatico, è sottoscritto con firma elettronica qualificata o firma digitale da chi presiede l'udienza e dal segretario. Nei casi in cui è richiesto, le parti procedono alla sottoscrizione delle dichiarazioni o del processo verbale apponendo la propria firma elettronica qualificata o firma digitale. 2. Qualora non sia possibile procedere alla sottoscrizione nella forma di cui a comma 1, il processo verbale viene redatto su supporto cartaceo, sottoscritto nei modi ordinari e acquisito al fascicolo informatico secondo le modalità di cui all'articolo 12".

Art. 16, D.M. 163/2013: "Redazione e deposito dei provvedimenti. 1. Ai fini della formazione delle sentenze, dei decreti e delle ordinanze, redatti come documenti informatici sottoscritti con firma elettronica qualificata o firma digitale dei soggetti di cui all'articolo 36, comma 3, del decreto legislativo 31 dicembre 1992, n. 546, la trasmissione dei documenti tra i componenti del collegio giudicante avviene tramite il S.I.Gi.T. 2. Il segretario di sezione sottoscrive, apponendo la propria firma elettronica qualificata o firma digitale, i provvedimenti di cui al comma 1, trasmessi tramite il S.I.Gi.T. e provvede al deposito della sentenza ai sensi dell'articolo 37 del decreto legislativo 31 dicembre 1992, n. 546".

[63] Per la consultazione della banca dati delle massime delle sentenze delle Commissioni Tributarie è possibile visualizzare il servizio di Documentazione Economica e Finanziaria sulla banca dati CERDEF in *https://def.finanze.it/DocTribFrontend/RS2_HomePage.jsp*.

Vale qui la pena sottolineare[64] che questa diversificazione normativa e pratica delle varie branchie processuali digitalizzate - anche nell'ambito dell'utilizzo dei provvedimenti giudiziari - ha fatto sorgere istanze di sensibilizzazione al Ministero della Giustizia evidenziando la necessità di realizzare un sistema di gestione dei diversi Processi Telematici oggi esistenti, attraverso l'implementazione di una piattaforma comune, caratterizzata da uniformità delle regole e delle specifiche tecniche, con la previsione del deposito telematico tramite Upload, piuttosto che a mezzo pec[65].

Risulta infatti opportuna, nell'ottica di velocizzazione dei processi - tanto cara al Legislatore ed all'opinione sociale - l'adozione di un'architettura informatica unica per tutti i settori[66].

2.1. Le sentenze digitali nel processo civile.

Sussistono vari aspetti del tema introdotto da approfondire nell'ambito del processo civile telematico, a cominciare dalle comunicazioni di cancelleria.

Con l'art. 16, comma 4, D.L. del 18 ottobre 2012, n. 179 è stato profondamente innovato il sistema delle comunicazioni di cancelleria dei provvedimenti, generalizzando l'obbligo della modalità telematica, da eseguire all'indirizzo pec risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, e sancendo espressamente la "*sanzione*" del deposito in cancelleria nell'ipotesi di mancato assolvimento all'obbligo di munirsi di un indirizzo pec (per i soggetti per i quali è prescritto) nonché nei casi di mancata consegna del messaggio pec per cause imputabili al destinatario (art. 16, comma 6, D.L. 179/2012)[67].

L'originaria modifica della formulazione dell'art. 133, comma 2, c.p.c. (con la previsione della comunicazione integrale del provvedimento, come modificato dall'art. 45, comma 1, lett. b, D.L. 24 giugno 2014, n. 90) aveva indotto gli interpreti

[64] Le ulteriori peculiarità, sin dalla fase di estrazione della copia digitale, saranno affrontate separatamente nei prossimi paragrafi.
[65] V. Comunicato stampa AIGA del 06.02.2020 – "*Upload, piattaforma comune per i riti telematici e messa in opera ppt*" in *https://aiga.it/comunicati/upload-piattaforma-comune-per-i-riti-telematici-e-messa-in-opera-ppt/*.
[66] V. anche il contributo di M. MIRIGLIANI "*Mozione sulla riorganizzazione della normativa in materia di processi telematici*" del 23.07.2021, presentata al XXXIV Congresso Nazionale Forense.
[67] In aderenza al dettato normativo, è stato quindi affermato che la mancata consegna all'avvocato della comunicazione o notificazione inviatagli a mezzo p.e.c. produce effetti diversi a seconda che gli sia o meno imputabile: nel primo caso, le notificazioni/comunicazioni saranno eseguite esclusivamente mediante deposito in cancelleria; nel secondo, attraverso l'utilizzo delle forme ordinarie previste dal codice di rito (Cass. 18 febbraio 2020, n. 3965).

a chiedersi se la "*mera*" comunicazione della cancelleria comportasse il decorso del termine breve per l'impugnazione anche della sentenza[68].

Per eliminare ogni dubbio, il legislatore è intervenuto in sede di conversione del D.L. 90/2014, aggiungendo al comma 2 dell'art. 133 c.p.c. un espresso chiarimento nel senso che "*La comunicazione non è idonea a far decorrere i termini per le impugnazioni di cui all'articolo 325*"[69]. Pertanto, in via generale, la comunicazione del provvedimento da parte della cancelleria non è idonea a far decorrere il termine breve per l'impugnazione, ma la modifica normativa non ha inciso sulle norme processuali, derogatorie e speciali, che collegano la decorrenza del termine breve di impugnazione alla mera comunicazione del provvedimento da parte della cancelleria[70].

Inoltre, l'art. 16-*sexies* del D.L. n. 179 del 2012[71], rubricato *Domicilio digitale*, ha successivamente statuito che, eccettuata l'ipotesi di cui all'art. 366 c.p.c., "*quando la legge prevede che le notificazioni degli atti in materia civile al difensore siano eseguite, ad istanza di parte, presso la cancelleria dell'ufficio giudiziario, alla notificazione con le predette modalità può procedersi esclusivamente quando non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo di posta elettronica certificata, risultante dagli elenchi di cui all'art. 6-bis d.lgs. 7 marzo 2005, n. 82, nonché dal registro generale degli indirizzi elettronici, gestito dal ministero della giustizia*"[72].

---

[68] I. FEDELE, *Ufficio del Massimario e del Ruolo – Processo Civile Telematico – rassegna tematica della giurisprudenza di legittimità* (aggiornato alle decisioni del 31.12.2020), in *Processo_civile_telematico_-_aggionata_al_31_12_2020.pdf*.

[69] Ai fini della decorrenza del termine cd. "lungo" di impugnazione è stato chiarito che, nel caso di redazione della sentenza in formato elettronico, non rileva il momento della trasmissione alla cancelleria da parte del giudice, bensì quello dell'attestazione del cancelliere, giacché è solo da tale momento che la sentenza diviene ostensibile agli interessati (Cass. 25 maggio 2020, n. 9546).

[70] Ad esempio, in tema di decorrenza del termine dalla comunicazione dell'ordinanza che dichiara l'inammissibilità dell'appello ai sensi dell'art. 348 *bis* c.p.c., è stato affermato che il disposto dell'art. 133, comma 2, c.p.c. non trova applicazione nel caso dell'art. 348 *ter*, comma 3, c.p.c., nella parte in cui fa decorrere il termine ordinario per proporre il ricorso per cassazione avverso il provvedimento di primo grado dalla comunicazione dell'ordinanza che dichiara l'inammissibilità dell'appello ai sensi dell'art. 348-*bis* c.p.c. (Cass. SS. UU. 15 dicembre 2015, n. 25208; Cass. 22 maggio 2017, n. 12780).

[71] Introdotto dall'art. 52, comma 1, lett. b), del D.L. 24 giugno 2014, n. 90, conv. in L. 11 agosto 2014, n. 114.

[72] Cass. 7 gennaio 2020, n. 93 ha poi ribadito che "*Ai sensi dell'art. 16 bis, comma 9 bis, del D.L. n. 179 del 2012, conv. in l. n. 221 del 2012, nel testo ratione temporis vigente, le copie informatiche del fascicolo digitale equivalgono all'originale, anche se prive della firma del cancelliere*" in quanto la predetta disposizione è applicabile a tutti gli atti digitalizzati contenuti nel fascicolo informatico, in tal modo respingendo un'eccezione di nullità di un'ordinanza, comunicata a mezzo PEC, perché priva della firma digitale del cancelliere.

Altro spunto interessante involge la sentenza digitale munita o meno di cosiddetta "*coccardina*".

In particolare, il dubbio che investe alcuni operatori del diritto è quello che attiene all'utilizzo della copia informatica (munita di coccarda e stringa grafica laterale) - piuttosto che del duplicato informatico - del provvedimento del Giudice da estrarre dal fascicolo informatico.[73]

Il duplicato informatico è definito dall'art. 1, lettera I *quinquies* del Codice dell'Amministrazione Digitale, come il *"il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario"* e, di conseguenza, si tratta a tutti gli effetti di un clone del file di origine.

In informatica, purtroppo, non è quasi mai possibile parlare di "originale" e "copia" come invece avviene per il cartaceo, e ciò proprio in virtù della definizione che è stata sopra evidenziata.

Un documento con la medesima sequenza binaria di un altro documento, infatti, sarà a tutti gli effetti non una copia ma un clone, o anche un secondo originale, poiché identico in tutto e per tutto al documento "*padre*".

Un duplicato informatico ricavato dal fascicolo digitale, quindi, avrà la medesima sequenza binaria del file presente sui server ministeriali ed includerà anche tutte le caratteristiche e le appendici del file medesimo, ivi compresa la firma digitale del magistrato[74].

La copia informatica scaricata dal fascicolo telematico, sempre a norma del CAD, può invece essere definita come "*il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari*"; quindi caratterizzato dal medesimo contenuto, ma con una differente sequenza binaria.

---

[73] Art. 23 *bis*, D. Lgs. del 7 marzo 2005, n. 82 – CAD "Duplicati e copie informatiche di documenti informatici 1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71. 2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico".

[74] Medesimo discorso va fatto per tutti gli atti presenti nel fascicolo telematico, quindi anche quelli caricati dall'avvocato.

Di fatto, sul duplicato informatico non apparirà alcuna "coccarda" e stringa grafica laterale, senza per questo poter essere definito un *minus* rispetto alla copia informatica, per quanto detto in precedenza, potendo essere indifferentemente estratto al fine della notifica (cartacea o telematica che sia).

La differenza attiene piuttosto all'apposizione dell'attestazione di conformità in calce all'atto cartaceo o da inserire all'interno della relata digitale. Difatti, il duplicato informatico non necessiterà di alcuna attestazione di conformità da inserire nella relata di notificazione per essere considerato di equivalente valore rispetto al documento "padre", mentre la copia informatica andrà invece attestata conforme a norma dell'art. 16 *bis*, comma 9 *bis*, D.L. 179/2012[75].

Quanto ai dubbi sulla sottoscrizione digitale della sentenza, in ogni caso, la Suprema Corte ha recentemente statuito che la coccarda e la stringa grafica sulla sentenza fanno desumere l'apposizione della firma digitale ad opera del giudice, fino a querela di falso, anche in quanto il sistema informatico impedisce il deposito telematico del documento non firmato digitalmente e comunque non genera la copia recante i segni grafici attestanti la presenza di una firma digitale.[76]

Sotto altro profilo, è attuale approfondire la tematica dell'estrazione ed utilizzo della copia della sentenza telematica.

Con particolare riguardo agli ultimi anni, se da un lato i giudizi innanzi ai Tribunali erano già da tempo caratterizzati dalla totale digitalizzazione, tali procedimenti non erano stati interessati dalla medesima procedura per l'estrazione di copie

[75] L. SILENI, *Che differenza c'è tra copia informatica e duplicato informatico nel PCT?*, in *Sistemiamo l'Italia*, in *https://www.sistemiamolitalia.it/faq/che-differenza-ce-tra-copia-informatica-e-duplicato-informatico-nel-pct/*.

[76] Cass. ord. 29 aprile 2021, n. 11306. Il ricorrente aveva denunciato la nullità della sentenza per mancanza/insufficienza della sottoscrizione in calce alla sentenza da parte del presidente del collegio così come da parte del giudice relatore. La Corte dichiara infondato tale motivo. Nel caso di specie, infatti, che la sentenza impugnata era stata redatta dalla Corte d'Appello di Venezia in formato elettronico e sottoscritta digitalmente sia dal giudice relatore sia dal presidente del collegio si desumeva, fino a querela di falso (*ex* art. D.Lgs. del 7 marzo 2005, n. 82, C.D.A.; cfr. Cass. del 19 giugno 2017, n. 15074), dalla riscontrata presenza della coccarda e della stringa apposte su ogni pagina della copia analogica del documento informatico con cui è stata redatta la sentenza impugnata. Infatti, dalle specifiche tecniche di cui al D.M. 21 febbraio 2011, n. 44 si desume che, in caso di mancanza della firma digitale, il sistema informatico impedisce il deposito telematico del documento e comunque non genera la copia recante i segni grafici attestanti la presenza di una firma digitale (coccarda e stringa). Pertanto, la Corte ha rigettato il motivo, ribadendo che la sentenza redatta in formato elettronico dal giudice e da questi sottoscritta con firma digitale, ai sensi dell'art. 15 D.M. cit., non è affetta da nullità per difetto di sottoscrizione, attesa l'applicabilità al processo civile e ai documenti informatici nell'ambito dello stesso emanati del c.d. Codice dell'amministrazione digitale (cfr. Cass. del 10 novembre 2015, n. 22871). Commento di S. M. MIRANDA in *Il foglio del consiglio*, 2021, in https://www.ilfogliodelconsiglio.it/giurisprudenza/coccarda-e-stringa-grafica-sulla-sentenza-fanno-desumere-l%E2%80%99apposizione-della-firma-digitale-ad-opera-del-giudice-cass-sez-i-ord-29-aprile-2021-n-11306/.

esecutive dei provvedimenti emessi. L'assenza di uno strumento volto ad ovviare alla necessità di provvedere alle richieste ed all'estrazione di dette copie da parte dei legali si è resa improrogabile con l'avvento della pandemia del Covid-19, che ne ha accelerato l'utilizzo[77].

Inizialmente, in assenza di una previsione legislativa ed a seguito di proposte dei vari Consigli degli Ordini e Corti d'Appello, si è cercato di trovare una soluzione tale da consentire l'estrazione di copie munite di formula esecutiva senza dover accedere alle cancellerie[78].

Ebbene, a seguito della forte spinta degli operatori del settore giustizia, in data 18.12.2020 il legislatore – in sede di conversione – ha introdotto il comma 9 *bis* all'art. 23 del D.L. 137/2020 (avvenuto con l. 176/2020)[79].

Tale previsione consente al difensore di richiedere la copia esecutiva della sentenza attraverso una istanza da depositare direttamente nel fascicolo telematico di interesse e proprio nel fascicolo telematico viene anche rilasciata, così che il titolo esecutivo potrà essere autenticato con attestazione di conformità direttamente dal difensore ai sensi dell'art. 16 *bis*, co. 9, D.L. 179/2012 e ss..

Tale attestazione sarà posta in calce all'atto scaricato o nel corpo della relata di notificazione, a seconda che si esegua una notifica cartacea o a mezzo pec.

---

[77] M. BONETTI, *Il processo amministrativo telematico e da remoto*, 2021, pp. 124-129.

[78] V. tra tutti, il *Protocollo di intesa per l'individuazione delle modalità di richiesta e rilascio dei titoli esecutivi* sottoscritto tra il COA di Roma e la Corte d'Appello di Roma il 01.12.2020, proprio al fine di contenere l'epidemia da Covid-19 e regolamentare gli accessi degli Avvocati al Palazzo di Giustizia. Tale accordo era stato preceduto da apposito quesito al Ministero della Giustizia che, con nota prot. n. 168232 del 15.10.2020 aveva riconosciuto l'utilizzabilità del rilascio di formula esecutiva in formato telematico e firmata digitalmente dal cancelliere, previo pagamento telematico dei relativi diritti di cancelleria.

[79] Art. 23, comma 9 *bis*, del D.L. 137/2020: "*La copia esecutiva delle sentenze e degli altri provvedimenti dell'autorità giudiziaria di cui all'articolo 475 del codice di procedura civile può essere rilasciata dal cancelliere in forma di documento informatico previa istanza, da depositare in modalità telematica, della parte a favore della quale fu pronunciato il provvedimento. La copia esecutiva di cui al primo periodo consiste in un documento informatico contenente la copia, anche per immagine, della sentenza o del provvedimento del giudice, in calce ai quali sono aggiunte l'intestazione e la formula di cui all'articolo 475, terzo comma, del codice di procedura civile e l'indicazione della parte a favore della quale la spedizione è fatta. Il documento informatico così formato è sottoscritto digitalmente dal cancelliere. La firma digitale del cancelliere tiene luogo, ai sensi dell'articolo 24, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, del sigillo previsto dall'articolo 153, primo comma, secondo periodo, delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie, di cui al regio decreto 18 dicembre 1941, n. 1368. Il difensore o il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio possono estrarre dal fascicolo informatico il duplicato e la copia analogica o informatica della copia esecutiva in forma di documento informatico. Le copie analogiche e informatiche, anche per immagine, della copia esecutiva in forma di documento informatico estratte dal fascicolo informatico e munite dell'attestazione di conformità a norma dell'articolo 16-undecies del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, equivalgono all'originale*".

Nel caso particolare di richiesta di esecutorietà e relativa formula esecutiva conseguente alla notifica del ricorso per decreto ingiuntivo non provvisoriamente esecutivo, l'avvocato dovrà anche allegare il ricorso ed il decreto notificato nonché la prova del perfezionamento con le relative ricevute.

Tuttavia, l'intervento legislativo non modifica l'art. 475 c.p.c. ma rappresenta una legislazione temporanea e d'urgenza.

Inizialmente è stato controverso il pagamento dei diritti di cancelleria, che variava tra Uffici Giudiziari, sino alla nota n. 0024495.U del 04.02.2021 del Ministero della Giustizia, il quale, a seguito delle richieste di chiarimento dei vari Uffici, ha sancito che "*gli uffici giudiziari dovranno, nell'arco temporale previsto dalla norma, rilasciare le copie esecutive con modalità telematica senza richiedere il versamento dei diritti di copia previsti dal D.P.R. n. 115 del 2002*".

2.2. I provvedimenti emessi dalla Corte di Cassazione e dal Giudice di Pace.

Interessante è anche la giurisprudenza che definisce l'ambito di utilizzo del provvedimento telematico nei giudizi per cassazione.

Per cominciare, è utile ribadire che ai fini del deposito della decisione in copia autentica nel ricorso per cassazione, ai sensi dell'art. 369, comma 2, n. 2., c.p.c., il difensore può giovarsi del potere di autentica di cui all'art. 16-*bis*, comma 9-*bis*, del D.L. n. 179 del 2012[80].

Quanto al soggetto legittimato ad eseguire tale attestazione di conformità, la competenza è del difensore che ha assistito la parte nel precedente grado di giudizio, "*i cui poteri processuali e di rappresentanza permangono, anche nel caso in cui allo stesso fosse stata conferita una procura speciale per quel singolo grado, sino a quando il cliente non conferisca il mandato alle liti per il giudizio di legittimità ad un altro difensore*"[81].

[80] V. Cass. 8 novembre 2017, n. 26479, secondo cui l'ambito del potere di autentica conferito ai difensori e dagli altri soggetti ivi indicati si estende a tutti gli atti e provvedimenti contenuti nel fascicolo informatico, sia perché originariamente depositati in formato digitale sia perché depositati in formato cartaceo e successivamente digitalizzati dal cancelliere, ai sensi dell'art. 15, comma 4, del D.M. 44/2011, senza circoscrivere l'applicabilità della norma ai soli procedimenti iscritti successivamente al 30 giugno 2014. Sulla necessità dell'attestazione di conformità *ex* art. 16 *bis*, comma 9 *bis*, del D.L. n. 179 del 2012, cit., per autenticare la copia della decisione impugnata, si esprime anche Cass. 29 novembre 2017, n. 28473.
[81] Cass. 8 maggio 2018, n. 10941, la include espressamente.

Di conseguenza, a seguito della nomina del difensore in cassazione, l'autenticazione della copia della sentenza d'appello - ai fini del ricorso - non può essere effettuata da un altro avvocato cui non sia stata conferita la procura speciale per la proposizione del suddetto ricorso, essendo solo il primo, sulla base della procura rilasciatagli per il giudizio di legittimità, abilitato all'attività di accesso presso il giudice della sentenza impugnata, al fine di ottenere la copia della sentenza dalla cancelleria o di acquisire le credenziali per l'accesso al fascicolo telematico[82].

Nell'ipotesi di notifica telematica del provvedimento impugnato, Cass. 22 dicembre 2017, n. 30765, ha sostenuto che "*In tema di ricorso per cassazione, qualora la notificazione della sentenza impugnata sia stata eseguita con modalità telematiche, per soddisfare l'onere di deposito della copia autentica della decisione con la relazione di notificazione, il difensore del ricorrente, destinatario della suddetta notifica, deve estrarre copia cartacea del messaggio di posta elettronica certificata pervenutogli e dei suoi allegati (relazione di notifica e provvedimento impugnato), attestare con propria sottoscrizione autografa la conformità agli originali digitali della copia formata su supporto analogico, ai sensi dell'art. 9, commi 1 bis e 1 ter, l. n. 53 del 1994, e depositare nei termini quest'ultima presso la cancelleria della S.C., mentre non è necessario provvedere anche al deposito di copia autenticata della sentenza estratta dal fascicolo informatico*".

Anche nel caso in cui il difensore depositi tempestivamente una copia semplice, priva di attestazione di conformità ovvero con attestazione non sottoscritta, "*l'improcedibilità può evitata ove il controricorrente non ne contesti la conformità ovvero il ricorrente provveda ad effettuare l'asseverazione "ora per allora"*"[83]. Tuttavia, per l'operatività di tali meccanismi "in sanatoria", è richiesto che ricorra il presupposto giustificativo dell'ambiente digitale, situazione ravvisabile nei casi di:

[82] V. Cass. 29 novembre 2018, n. 30846. In senso conforme, Cass. 11 marzo 2020, n. 6907, che ha dichiarato improcedibile il ricorso nel caso dell'attestazione di conformità della sentenza impugnata redatta dal difensore in grado di appello successivamente al conferimento della procura speciale per il ricorso per cassazione ad altro difensore.

[83] Cass. SS. UU. 24 settembre 2018, n. 22438. I principi così affermati hanno trovato immediata applicazione da parte delle sezioni semplici (v., ad esempio, Cass. 19 aprile 2019, n.11102; conforme, Cass. 21 gennaio 2020, n. 1147), anche nel senso di dichiarare l'improcedibilità del ricorso ove non risultino applicabili i meccanismi in sanatoria elaborati dalle Sezioni Unite, con particolare riferimento alla mancata costituzione delle parti intimate in assenza di asseverazione di conformità della copia della decisione impugnata (Cass. 14 febbraio 2020, n. 3715; v. anche Cass. 12 giugno 2020, n. 11383, relativa ad un caso in cui l'asseverazione, proveniente dal difensore del ricorrente nel giudizio di merito, non era stata dallo stesso sottoscritto, rendendo inefficace l'attestazione).

a) sentenza impugnata redatta in formato elettronico e firmata digitalmente, necessariamente inserita nel fascicolo informatico; b) sentenza impugnata sottoscritta con firma autografa ed inserita nel fascicolo informatico; c) deposito di provvedimento comunicato dalla cancelleria a mezzo pec.

Va poi precisato che la notifica della sentenza di Cassazione effettuata alla controparte a mezzo pec *ex* art. 3 *bis* della L. 53/1994 è idonea a far decorrere il termine breve d'impugnazione nei confronti del destinatario, ove il notificante provi di aver allegato e prodotto la copia cartacea del messaggio di trasmissione a mezzo posta elettronica certificata, le ricevute di avvenuta consegna e accettazione e la relata di notificazione, sottoscritta digitalmente dal difensore, nonché la copia conforme della sentenza che, trattandosi di atto da notificare non consistente in documento informatico, sia stata effettuata mediante estrazione di copia informatica dell'atto formato su supporto analogico e attestazione di conformità *ex* art. 16 *undecies* del citato D.L. n. 179/2012[84].

In ogni caso, vale il principio di raggiungimento dello scopo ove l'interessato non alleghi il pregiudizio subito per effetto di tale violazione, anche in mancanza dall'attestazione di conformità delle ricevute di avvenuta consegna e accettazione del messaggio, poiché è possibile far decorrere il termine breve d'impugnazione nei confronti del destinatario qualora quest'ultimo non abbia sollevato alcuna obiezione o contestazione sulla regolarità di tale notifica[85].

---

[84] Cass. 19 settembre 2017, n. 21597; in senso conforme, Cass. 26 giugno 2018, n. 16783, Cass. 5 ottobre 2018, 24568, Cass. 9 luglio 2019, n. 18317 - Annotata da F. PEDRONI, *Gli oneri probatori dell'avvenuta notifica in proprio a mezzo PEC ai fini della decorrenza del termine breve di impugnazione,* in *ilprocessotelematico.it, 2019.* Tuttavia, in un caso in cui era stata contestata la regolarità dell'estrazione della copia su supporto analogico, è stata esclusa la tardività del ricorso per cassazione (dedotta dal controricorrente con riferimento ad una prima notifica effettuata a mezzo PEC) in quanto, a seguito delle contestazioni, il notificante aveva proceduto ad una seconda notifica, con conseguente decorrenza del termine per impugnare dalla data di quest'ultima (Cass. 19 giugno 2019, n. 16421).

[85] Cass. 28 novembre 2017, n. 28339. Nel caso di specie, in cui la sentenza impugnata risultava notificata dapprima a mezzo pec e poi, nuovamente, a mezzo ufficiale giudiziario, la Corte ha ritenuto che il termine di cui all'art. 325, comma 2, c.p.c. decorresse dalla prima notifica, pur in assenza di attestazione di conformità delle ricevute di avvenuta consegna della stessa, essendosi il ricorrente, a fronte dell'eccezione di tardività del ricorso con deposito della documentazione attestante l'avvenuta notifica a mezzo pec, limitato a richiamare in memoria la seconda notificazione, senza nulla obiettare sulla regolarità della prima. In senso analogo, Cass. 16 agosto 2018, n. 20747, ha affermato che la notificazione telematica della sentenza, mediante copia priva della regolare attestazione di conformità all'originale, ma la cui relata contenga l'indicazione della data di pubblicazione e l'attestazione che la stessa, originariamente, recava firma digitale, è idonea a far decorrere il termine breve per l'impugnazione, salvo che il destinatario deduca e dimostri che tale irregolarità abbia arrecato un pregiudizio alla conoscenza dell'atto ed al concreto esercizio del diritto di difesa.

Resta, peraltro, a carico del destinatario della notifica non solo l'onere di contestazione, ma anche di prova della mancata ricezione della sentenza o del provvedimento oggetto della notificazione[86].

In relazione, invece, al giudizio innanzi al Giudice di Pace è il caso di evidenziare che - essendo ancora inefficace la disciplina del processo telematico - in assenza della normativa ministeriale, è necessario estrarre copie analogiche degli atti digitali ed attestarne la conformità, in virtù del potere appositamente conferito al difensore dagli artt. 6 e 9, commi 1-*bis* e 1-*ter*, della l. n. 53 del 1994[87].

È pacifica, invece, l'idoneità della notifica a mezzo pec della sentenza del Giudice di Pace (per scansione dell'originale informatico conforme) ai fini della decorrenza del termine breve per l'impugnazione, sussistendo il potere di autentica del difensore, ai fini della notifica a mezzo pec, sebbene non esista materialmente un fascicolo informatico da cui estrarre il provvedimento, dal momento che il provvedimento può essere rilasciato in copia conforme dalla cancelleria e, poi, in un momento successivo, allegato al messaggio pec e attestato conforme dal difensore notificante ai sensi dell'art. 3-*bis*, comma 2, della legge n. 53 del 1994[88].

3. Le sentenze nel processo tributario.

Con l'introduzione del PTT[89] è possibile estrarre dal fascicolo informatico anche le copie dei provvedimenti del Giudice, in esenzione del pagamento dei diritti di copia semplice[90].

Le parti processuali per poter utilizzare le funzionalità dell'estrazione della sentenza devono accedere al sistema tramite il portale della giustizia tributaria *www.giustiziatributaria.gov.it*.

---

[86] Cass. 31 ottobre 2017, n. 25819 e Cass. 24 settembre 2020, n. 20039.
[87] Cass. 29 settembre 2020, n. 20575, che ha osservato come il deposito degli atti dinanzi gli uffici dei Giudici di Pace non possa avvenire mediante posta elettronica certificata o, come nel caso di specie, mediante invio di raccomandata on line ai server delle Poste Italiane.
[88] Cass. 19 luglio 2019, n. 19517 - Annotata da S. CAPRIO, *Idoneità della notifica a mezzo pec della sentenza del giudice di pace ai fini della decorrenza del termine breve*, in *ilprocessotelematico.it*, 2019.
[89] Nel 2011 sono state poste le premesse normative per una progressiva digitalizzazione del processo tributario. In particolare, l'art. 39 del D.L. 98/2011, convertito dalla L. 111/2011, ha introdotto specifiche disposizioni per una completa informatizzazione del processo tributario telematico, anche in attuazione dei principi previsti dal codice dell'amministrazione digitale. Si sono poi susseguiti il D.M. 23 dicembre 2013, n. 163, con rinvio della concreta attuazione della digitalizzazione delle varie fasi del processo ai decreti attuativi di adozione delle regole tecniche.
[90] V. Circolare del Dipartimento delle Finanze n. 1 del 4 luglio 2019.

L'accesso al fascicolo, tramite la funzione "Telecontenzioso", permette di visualizzare le informazioni sui ricorsi depositati, lo stato del processo e gli atti presenti nel fascicolo.

In particolare, l'utente può consultare, oltre agli atti depositati dalle parti (ad es. ricorso, memorie, controdeduzioni), anche i provvedimenti emanati dal giudice[91].

Oltre alla visione e consultazione degli atti e dei documenti è, inoltre, possibile estrarre copia degli stessi in esenzione dal pagamento dei diritti di copia, in base all'art. 269 del T.U. n. 115/2002, per poi poter utilizzare tali copie sia per la notifica delle stesse alle controparti che per uso appello.

A tale riguardo, l'art. 16 del D.L. 119/2018, ha introdotto apposite disposizioni riguardanti la digitalizzazione del processo tributario stabilendo, tra l'altro, a decorrere dal 24.10.2018, che i difensori delle parti, degli enti impositori e dei soggetti della riscossione possono attestare la conformità agli originali o copia conforme della copia analogica o digitale degli atti prelevati dal fascicolo processuale informatico o ricevuti tramite notifica telematica ovvero detenuti in originale o in copia conforme, sulla base delle nuove disposizioni contenute nell'articolo 25-*bis* del D.Lgs. n. del 31 dicembre 1992, n. 546[92], introdotto dall'articolo 16, comma 1, lettera b) del D.L. 119/2018.

Spetta, altresì, all'Ufficio di segreteria della Commissione tributaria competente l'attestazione del passaggio in giudicato della sentenza ai sensi dell'art. 124 disp. att. c.p.c., che verrà posta sul provvedimento già notificato a mezzo pec alla controparte, stampato e dichiarato conforme all'originale ai sensi dell'art. 16, comma 3, del D.L. n. 119/2018. Resta fermo il pagamento dei diritti di copia autentica e di certificazione sulle copie rilasciate dalla segreteria della Commissione.

---

[91] Si precisa che le fasi processuali interamente telematizzate nel processo tributario sono quelle della notifica, della costituzione in giudizio e del deposito degli atti processuali, oltre che della consultazione del fascicolo processuale. Restano da digitalizzare i provvedimenti adottati dal giudice tributario ed il verbale d'udienza.
Si tratta di atti formati in originale analogico che sono scansionati e firmati digitalmente dal personale dell'Ufficio di segreteria delle Commissioni tributarie per poi essere inseriti fascicolo informatico.

[92] In particolare, il comma 1 del suddetto articolo 25 *bis* dispone che i difensori pubblici e privati al momento del deposito degli atti possono attestare la conformità delle copie degli atti digitali a quelli analogici detenuti in originale o in copia conforme, allegando a dette copie un'apposita dichiarazione secondo le modalità previste dal D.Lgs. n. 82/2005. Inoltre, il successivo comma 2 prevede analogo potere per i difensori quando estraggono gli atti e provvedimenti presenti nel fascicolo informatico o trasmessi in allegato alle comunicazioni telematiche dell'Ufficio di Segreteria. La copia dichiarata conforme e firmata digitalmente equivale all'originale. Non sono dovuti i diritti di copia autentica.

Si precisa inoltre che, le modifiche apportate dal D.Lgs. n. 156/2015 alla disciplina del processo tributario di cui al D.Lgs. 546/92 – eliminando il riferimento all'applicabilità in via sussidiaria delle disposizioni del codice di procedura civile – prevedono il giudizio di ottemperanza, nell'attuale formulazione di cui all'art. 70, D.Lgs. n. 546/92, quale unico rimedio esperibile in materia di esecuzione coattiva delle sentenze tributarie, ancorché non definitive.

Per attivare il giudizio di ottemperanza, quindi, non è più necessario il rilascio di copia della sentenza in forma esecutiva.

Come già precisato, quanto alla notifica a mezzo pec, si utilizza la copia della sentenza estratta dal fascicolo telematico, la quale deve essere sottoscritta digitalmente dal difensore che in tal modo ne attesta la conformità all'originale. A tal fine, si dovrà indicare nell'oggetto che si sta procedendo alla notifica di sentenza ai sensi dell'art. 38 del D.Lgs. 546/1992.

Si ritiene, inoltre, possibile predisporre la relata di notifica, benché non sia necessaria, in considerazione della particolarità del contenzioso tributario che permette la notifica sia con consegna a mani, che a mezzo posta con raccomandata e ricevuta di ritorno (quindi senza che sia necessario predisporre la relata di notifica). Nel testo della pec si potrà indicare che si tratta di notifica ai sensi dell'art. 16-*bis* co. 3 del DLgs. 546/92[93].

Entro 30 giorni dalla notifica, è necessario depositare la copia autentica notificata unitamente alla copia del messaggio di pec predisposto per la notifica della sentenza, ed alle ricevute di invio e di accettazione rilasciate dal sistema a seguito dell'invio della pec; in mancanza decorrerà il termine di impugnazione ordinario semestrale di cui all'art. 327 c.p.c..

4. Le sentenze nel processo amministrativo.

Come premesso, il PAT[94] ha obbligato anche i magistrati a redigere e depositare i loro atti sotto forma di documento informatico sottoscritto con firma digitale, a

[93] A. CISSELLO, C. MONTELEONE E C. RUFFINO, *Il processo tributario telematico - Analisi degli aspetti operativi del processo tributario telematico, obbligatorio per i ricorsi di primo e secondo grado notificati dall'1.7.2019*, in *spei8_-_giugno_2019_odcec_2.pdf*.

[94] Dal 1° gennaio 2017, dopo una lunga attesa costellata da semestrali rinvii, il processo amministrativo telematico è stato reso esecutivo. M. REALE, in *Processo Amministrativo Telematico, un vademecum per i Colleghi Avvocati*, 2017, in *https://www.altalex.com/documents/news/2017/01/09/processo-amministrativo-telematico-un-vademecum-per-i-colleghi-avvocati*.

differenza di quanto ad oggi previsto nel processo civile telematico dove il magistrato deve redigere e depositare obbligatoriamente in modalità telematica solo il decreto a seguito del ricorso per decreto ingiuntivo[95].

Il comma 3 dell'art. 7 delle regole tecniche[96] prevede poi che il deposito del documento redatto su supporto cartaceo e sottoscritto con firma autografa è consentito esclusivamente quando il Responsabile del SIGA attesta che il sistema informatico non è in grado di ricevere il deposito telematico degli atti. In tal caso, il Segretario di sezione provvede ad estrarre copia informatica, anche per immagine, dei provvedimenti depositati e, dopo averne attestata la conformità all'originale con firma digitale, la inserisce nel fascicolo informatico.

I magistrati utilizzano per la redazione ed il deposito dei provvedimenti giurisdizionali in formato digitale il sistema denominato "*Scrivania del magistrato*", consistente in un'applicazione software inserita su supporto rimovibile e protetto ed i provvedimenti vengono redatti quali documenti informatici, in formato PDF ("testo"), ottenuto dalla trasformazione di documento testuale, sottoscritto con firma digitale in formato "PAdES"[97].

Come nel processo civile, con la modifica apportata dalla l. del 25 ottobre 2016, n. 197, al comma 2 *ter* all'articolo 136 del codice del processo amministrativo è attribuito al difensore lo stesso potere di attestazione in quanto la citata norma adesso prevede che *"Analogo potere di attestazione di conformità è esteso agli atti e ai provvedimenti presenti nel fascicolo informatico, con conseguente esonero dal versamento*

---

[95] M. REALE, in *Le regole e le specifiche tecniche del PAT: prime considerazioni*, 2016, in *https://maurizioreale.it/le-regole-e-le-specifiche-tecniche-del-pat-prime-considerazioni*.

[96] D.P.C.M. del 16 febbraio 2016, n. 40 - Regolamento recante le regole tecnico-operative per l'attuazione del processo amministrativo telematico. Art. 7 Provvedimenti del giudice: 1. I provvedimenti del giudice sono redatti e depositati sotto forma di documento informatico sottoscritto con firma digitale. I provvedimenti collegiali sono redatti dall'estensore, da questi sottoscritti e trasmessi telematicamente al presidente del collegio, che li sottoscrive e li trasmette telematicamente alla Segreteria per il deposito. 2. Il Segretario di sezione sottoscrive con la propria firma digitale i provvedimenti di cui al comma 1, provvede al loro deposito nel fascicolo informatico e alla contestuale pubblicazione, mediante inserimento, nel SIGA e sul sito INTERNET della giustizia amministrativa, con le cautele previste dalla normativa in materia di tutela dei dati personali, ed in particolare nel rispetto della disciplina dettata dagli articoli 51 e 52 del Codice dei dati personali, secondo le modalità stabilite dalle specifiche tecniche di cui all'articolo 19. 3. Il deposito del documento redatto su supporto cartaceo e sottoscritto con firma autografa è consentito esclusivamente quando il Responsabile del SIGA attesta che il sistema informatico non è in grado di ricevere il deposito telematico degli atti. In tal caso, il Segretario di sezione provvede ad estrarre copia informatica, anche per immagine, dei provvedimenti depositati, nei formati stabiliti dalle specifiche tecniche di cui all'articolo 19 e la inserisce nel fascicolo informatico. 4. Il deposito dei provvedimenti con modalità informatiche sostituisce, ad ogni effetto, il deposito con modalità cartacee.

[97] Art. 136 *bis* c.p.a.: *Salvi i casi di cui al comma 2, tutti gli atti e i provvedimenti del giudice, dei suoi ausiliari, del personale degli uffici giudiziari e delle parti sono sottoscritti con firma digitale.*

dei diritti di copia. Resta escluso il rilascio della copia autentica della formula esecutiva ai sensi dell'articolo 475 del codice di procedura civile, di competenza esclusiva delle segreterie degli uffici giudiziari. La copia munita dell'attestazione di conformità equivale all'originale o alla copia conforme dell'atto o del provvedimento. Nel compimento dell'attestazione di conformità di cui al presente comma i difensori assumono ad ogni effetto la veste di pubblici ufficiali".

Quanto alle notificazioni a mezzo pec delle sentenze amministrative, alla pari dei relativi ricorsi, dopo un primo periodo controverso sull'ammissibilità o meno delle notifiche tramite pec *ex* L. 53/1994[98], è oramai pacifico l'utilizzo di tale modalità di notificazione alla stregua del civile, per cui valgono le medesime considerazioni.

Il Consiglio di Stato, sezione terza, con la sentenza del 14 settembre 2015, n. 4270 ha, difatti, definitivamente riconosciuto la validità della notifica tramite pec nel processo amministrativo[99].

Quanto alla richiesta delle copie esecutive dei provvedimenti nel processo amministrativo, almeno per il momento le stesse vengono fornite soltanto mediante consegna di copia cartacea dietro pagamento dei relativi diritti, previo deposito dell'istanza digitale nel fascicolo telematico attraverso l'inoltro telematico del modulo deposito richieste alla segreteria[100].

Ad oggi, sebbene il rinvio *ex* art. 39 c.p.a.[101] alle disposizioni del codice di procedura civile, non si può operare infatti il rinvio esterno stante l'esistenza di una disposizione specifica, quale l'art. 136, co. 2, *ter* del c.p.a. recante "*Disposizioni sulle comunicazioni e sui depositi informatici*".

---

[98] M. REALE, in *Notifiche PEC nel processo amministrativo: tutte le sentenze, 2015*, in *https://www.cedam.com/notifiche_pec_nel_processo_amministrativo_tutte_le_sentenze_id1171585_art.aspx*. Il TAR Lazio, terza sezione *ter*, con la sentenza del 13 gennaio 2015, n. 396, ha fatto proprie le considerazioni contenute nell'ordinanza del Consiglio di Stato 10 dicembre 2014, n. 33, adunanza plenaria ed ha, conseguentemente, dichiarato l'inammissibilità del ricorso notificato ai sensi della Legge 53/94 affermando che nel processo amministrativo allo stato non sarebbe possibile utilizzare tale modalità di notifica ove il difensore non abbia richiesto e ottenuto la prevista autorizzazione da parte del Presidente del TAR ai sensi dell'art. 52, comma 2, c.p.a.

[99] È stato affermato che la mancata autorizzazione presidenziale *ex* art. 52, co. 2, del c.p.a. non può considerarsi ostativa alla validità ed efficacia della notificazione dell'atto a mezzo p.e.c. atteso che nel processo amministrativo trova applicazione immediata la l. n. 53/1994 (ed in particolare gli articoli 1 e 3 *bis* della legge stessa), nel testo modificato dall'art. 25 co. 3, lett. a) della l. 12 novembre 2011, n. 183, secondo cui l'avvocato "*può eseguire la notificazione di atti in materia civile, amministrativa e stragiudiziale (...) a mezzo della posta elettronica certificata*".

[100] M. BONETTI, *Il processo amministrativo telematico e da remoto*, 2021, in *https://www.avvocatomichelebonetti.it/notizie/il-processo-amministrativo-telematico-e-da-remoto-manuale-a-cura-di-m-bonetti-con-la-collaborazione-di-c-palladino-b-colella-t-sesti*, pp. 129-131.

[101] Secondo cui le disposizioni del codice di procedura civile si applicano "*per quanto non disciplinato dal presente codice*".

La citata disposizione – nel prevedere la possibilità per i difensori di estrarre dal fascicolo informatico copia degli atti e provvedimenti ivi contenuti (che munita della debita attestazione di conformità equivale all'originale e alla copia conforme del provvedimento), con conseguente esonero dei diritti di copia – espressamente esclude "*il rilascio della copia autentica della formula esecutiva ai sensi dell'art. 475 c.p.c. di competenza esclusiva delle segreterie degli uffici giudiziari*".

Essa, quindi, non fa trovare applicazione all'art. 23 comma 9-*bis* del D.L. n. 137/2020 (conv. in l. n. 176/2020), almeno allo stato, nel processo amministrativo.

Tra l'altro, tale interpretazione è stata esplicitata anche dal Presidente del T.A.R. Campania con nota n. 424 del 29.01.2021, alla quale ha aderito anche il Presidente del Consiglio di Stato, con cui è stato chiarito che spetta alla segreteria del TAR il rilascio della copia autentica, in risposta a specifica richiesta avanzata dal COA Napoli l'11.01.2021[102].

5. Note bibliografiche.

BONETTI M., *Il processo amministrativo telematico e da remoto*;

CAPRIO S., *Idoneità della notifica a mezzo pec della sentenza del giudice di pace ai fini della decorrenza del termine breve*;

CISSELLO A., MONTELEONE C. e RUFFINO C., *Il processo tributario telematico - Analisi degli aspetti operativi del processo tributario telematico, obbligatorio per i ricorsi di primo e secondo grado notificati dall'1.7.2019*;

FEDELE I., *Ufficio del Massimario e del Ruolo – Processo Civile Telematico – rassegna tematica della giurisprudenza di legittimità*;

MIRANDA S. M., *Il foglio del consiglio;*

MIRIGLIANI M., *Mozione sulla riorganizzazione della normativa in materia di processi telematici*;

[102] "*Formula esecutiva digitale: la previsione del D.l. Ristori si applica nel processo amministrativo?*", 2021, in *https://ilprocessotelematico.it/articoli/news/formula-esecutiva-digitale-la-previsione-del-dl-ristori-si-applica-nel-processo* – Redazione scientifica.

PEDRONI F., *Gli oneri probatori dell'avvenuta notifica in proprio a mezzo PEC ai fini della decorrenza del termine breve di impugnazione*;

PIANA D. - Justice-ER - Percorsi e strumenti per una giustizia digitale al servizio del cittadino;

REALE M., in *Notifiche PEC nel processo amministrativo: tutte le sentenze;*

REALE M., in *Processo Amministrativo Telematico, un vademecum per i Colleghi Avvocati;*

REALE M., in *Le regole e le specifiche tecniche del PAT: prime considerazioni*;

SILENI L., *Che differenza c'è tra copia informatica e duplicato informatico nel PCT?*, in *Sistemiamo l'Italia*;

Cass. 10 novembre 2015, n. 22871;

Cass. SS. UU. 15 dicembre 2015, n. 25208;

Cass. 22 maggio 2017, n. 12780;

Cass. 19 giugno 2017, n. 15074;

Cass. 19 settembre 2017, n. 21597;

Cass. 31 ottobre 2017, n. 25819;

Cass. 8 novembre 2017, n. 26479;

Cass. 28 novembre 2017, n. 28339;

Cass. 29 novembre 2017, n. 28473;

Cass. 22 dicembre 2017, n. 30765;

Cass. 8 maggio 2018, n. 10941;

Cass. 26 giugno 2018, n. 16783;

Cass. 16 agosto 2018, n. 20747;

Cass. SS. UU. 24 settembre 2018, n. 22438;

Cass. 5 ottobre 2018, 24568;

Cass. 29 novembre 2018, n. 30846;

Cass. 19 aprile 2019, n.11102;

Cass. 19 giugno 2019, n. 16421;

Cass. 9 luglio 2019, n. 18317;

Cass. 19 luglio 2019, n. 19517;

Cass. 7 gennaio 2020, n. 93;

Cass. 21 gennaio 2020, n. 1147;

Cass. 14 febbraio 2020, n. 3715;

Cass. 18 febbraio 2020, n. 3965;

Cass. 11 marzo 2020, n. 6907;

Cass. 25 maggio 2020, n. 9546;

Cass. 12 giugno 2020, n. 11383;

Cass. 24 settembre 2020, n. 20039;

Cass. 29 settembre 2020, n. 20575;

Cass. ord. 29 aprile 2021, n. 11306;

Consiglio di Stato 14 settembre 2015, n. 4270;

Consiglio di Stato 10 dicembre 2014, n. 33;

Comunicato stampa AIGA del 06.02.2020 – "*Upload, piattaforma comune per i riti telematici e messa in opera ppt*.

IL RAPPORTO TRA L'INTELLIGENZA ARTIFICIALE E I PRINCIPI FONDAMENTALI IN MATERIA PENALE: QUALI PROSPETTIVE?

di Michele Rendina

SOMMARIO: 1. Intelligenza artificiale: definizioni e prospettive. – 2. La Carta etica sull'utilizzo dell'intelligenza artificiale. – 3. La responsabilità penale degli agenti intelligenti. – 4. Gli strumenti di *law enforcement* (polizia predittiva). – 5. L'utilizzo degli algoritmi predittivi per valutare la pericolosità sociale (*risk assessment tools*). – 6. La giustizia predittiva (*automated decision systems*). – 7. Riflessioni conclusive.

Abstract: *Artificial intelligence pervades every area of our life and will do so more and more. However, in the criminal justice sector there may be significant critical issues in terms of fundamental human rights. These critical issues will have to be addressed and resolved by the supranational lawmaker and the domestic lawmaker, even if this will also entail a conflict between fundamental rights and the prospects for technological development of AI systems, and therefore of economic growth.*

1. Intelligenza artificiale: definizioni e prospettive.

L'intelligenza artificiale ormai pervade le nostre vite, probabilmente molto di più di quel che crediamo. Ha invaso la nostra quotidianità attraverso gli *smartphone*, gli elettrodomestici,i *videogame*, ed è impiegata stabilmente dalle società di assicurazioni, dalle banche, gli ospedali e i governi. Insomma, siamo circondati dall'intelligenza artificiale e si tratta di una tendenza destinata a crescere enormemente nei prossimi anni. Infatti, si stima che il mercatodell'IA possa raggiungere nel 2025 un valore pari a 300 miliardi di dollari, con una crescita annuale del 17%[103]. Questi dati ci raccontano della

[103] Cfr. Rapporto della I.D.C., IDC *"Forecasts Strong 12.3% Growth for AI Market in 2020Amidst Challenging Circumstances"*, agosto 2020 https://www.idc.com/getdoc.jsp?containerId=prUS46757920.

enorme espansione che avrà il mercato dell'IA, espansione che di certo non risparmierà il settore della giustizia penale.

Prima di affrontare le ripercussioni che l'intelligenza artificiale potrebbe avere sul settore della giustizia penale, dobbiamo innanzitutto chiederci cosa intendiamo esattamente per intelligenza artificiale.

Non esiste una definizione univoca di IA. Possiamo dire, citando la definizione coniata dal Consiglio d'Europa, che si tratta di "un insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano. Gli sviluppi attuali mirano, ad esempio, ad affidare a una macchina compiti complessi precedentemente delegati ad un essere umano"[104]. Tale definizione in qualche modo richiama quella coniata dal padre della intelligenza artificiale John McCarthy, il quale allo stesso modo immaginò una macchina capace di imitare/simulare le capacità cognitive umane[105]. Quest'insieme eterogeneo di strumenti mira asostituire o ad affiancare l'essere umano, inteso sia come singolo individuo, in riferimento alle più disparate attività della vita quotidiana, che come gruppo sociale, inserito nella vita collettiva della comunità.

Una definizione di intelligenza artificiale che può far comprendere meglio la complessità e l'ampiezza di tali tecnologie è stata predisposta dal AI HLEG, il gruppo di esperti in IA costituito dalla Commissione Europea, secondo cui "I sistemi di intelligenza artificiale (IA) sono sistemi software (e verosimilmente anche hardware) progettati da esseri umani che, dato un obiettivo complesso, agiscono all'interno di una dimensione fisica o digitale, percependo il loro ambiente attraverso l'acquisizione di dati, interpretando i dati raccolti, siano essi strutturati o non strutturati, ragionando sulla conoscenza, o elaborando le informazioni derivate da questi dati e selezionando tra tutte le azioni possibili le migliori per raggiungere l'obiettivo indicato. I sistemi di intelligenza artificiale possono utilizzare regole simboliche o apprendere un modello numerico e possono anche adattare il loro comportamento analizzando il modo in cui l'ambiente è influenzato dalle loro azioni passate"[106].

---

[104] Cfr. https://www.coe.int/en/web/human-rights-rule-of-law/artificial- intelligence/glossary.
[105] Cfr. J. KAPLAN, *"Intelligenza artificiale. Guida al futuro prossimo"*, Luiss University Press, II ed., 2018, p. 37.
[106] Cfr. U. RUFFOLO (a cura di), *"Intelligenza artificiale. Il diritto, i diritti, l'etica"* Milano, Giuffrè Francis Lefebvre, 2020, p. 63; v. anche AI-HLEG, High Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and Scientific Disciplines*, 2019.

Tutte queste definizioni, dunque, si soffermano sulla capacità dell'IA di sostituire o affiancare l'essere umano nelle sue attività. Per quanto riguarda la prospettiva di sostituzione della attività umana, autorevoli studiosi si mostrano preoccupati per gli sviluppi che potrebbero derivare dalla implementazione dell'IA, soprattutto se raffrontati agli sviluppi della robotica e dell'ingegneria genetica. In sostanza, secondo costoro vi è il pericolo che possa sorgere in futuro una vera e propria tecnocrazia, dominata da superuomini dopati dalla ingegneria genetica, o addirittura che possa il nostro mondo essere soggiogato da robot umanoidi, così intelligenti, da relegare l'essere umano ad entità di secondo livello, alla stregua del rapporto che noi umani abbiamo con i nostri animali domestici[107].

Altri autori ritengono invece che questa prospettiva distopica, non sia attualmente neppure una possibilità, o comunque si tratterebbe di una eventualità troppo difficile da realizzarsi,considerato lo stato dell'arte dell'IA e dei suoi attuali intrecci con l'ingegneria genetica. In particolare, si ritiene che la capacità delle "macchine intelligenti" di sostituirsi all'essere umano sia molto limitata. Da un lato, le macchine riescono, seppur talvolta con estrema efficienza ed efficacia, a svolgere solo singoli compiti o fasi di procedimenti più complessi, attraverso ad esempio tecniche di *machine learning* o di autoapprendimento. Dall'altro lato, le attuali conoscenze tecnologiche sono lontanissime dal riuscire ad implementare tali capacità cognitive in robot che abbiano le fattezze umane. La robotica, infatti, allo stesso modo della IA, ha limitate capacità di sostituzione dell'essere umano: a differenza dell'IA che si occupa per lo più della implementazione delle capacità cognitive, la robotica ottiene i suoi maggiori risultati in relazione alle attività manuali nel settore industriale, all'interno delle cosiddette catene di montaggio, sostituendo l'essere umano in attività che sarebbero troppo faticose da svolgere.

La distopia rappresentata dall'unione dello sviluppo della capacità cognitiva, dovuto alla intelligenza artificiale, allo sviluppo della capacità fisica e di movimento nello spazio dovuto alla robotica, coadiuvate entrambe dalla ingegneria genetica, è al momento da considerarsi impossibile da realizzare. Con gli standard tecnologici attuali sarebbe impossibile riprodurre nelle macchine intelligenti la sinergia che caratterizza il rapporto mente-corpo tipica dell'essere umano[108].

---

[107] Cfr. S. HAWKING, *"Brief Answers to the Big Questions",* Hachette Collections, 2018 e Y. N. HARARI, *"Homo Deus, breve storia del futuro"*, Milano, Bompiani, 2017, pp. 427 ss.
[108] Cfr. G. ALPA (a cura di), *"Diritto e Intelligenza Artificiale"*, Pisa, Pacini Giuridica Editore, 2020, pp. 23 – 33.

Dunque, l'intelligenza artificiale probabilmente non riuscirà a sostituire l'essere umano nelle sue attività più complesse, ma avrà certamente delle ripercussioni notevoli in tutti i settoridelle attività umane, tra questi il settore della giustizia penale.

2. La Carta etica sull'utilizzo dell'intelligenza artificiale.

Il rapporto tra la giustizia penale e l'intelligenza artificiale, a causa della potenziale pervasività di quest'ultima, appare meritevole di essere approfondito, per tutte le tensioni e le criticità che possono ravvisarsi, soprattutto nella prospettiva dei principi fondamentali della persona in materia penale.

L'esigenza di affrontare le predette criticità sono state certamente avvertite in ambito sovranazionale: in particolare è da segnalare la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, elaborata dalla Commissione Europea per l'Efficienza della Giustizia del Consiglio d'Europa (CEPEJ) adottata il 3 e 4 dicembre 2018, che tenta di approfondire in modo compiuto tutte le potenzialità applicative dell'IA nel settore della giustizia penale e le relative controindicazioni[109].

La Carta è indirizzata ai legislatori e agli operatori dei sistemi giudiziari nazionali e cerca di fornire, attraverso un insieme eterogeneo di disposizioni (soprattutto di *soft law*) delle linee guida che consentano di affrontare le sfide, presenti e future, poste dall'intelligenza artificiale, alla luce dei principi fondamentali della CEDU.

Nella parte introduttiva della Carta vi è un ampio spazio dedicato ai cinque principi cui deve ispirarsi l'utilizzo dell'intelligenza artificiale, in particolare parliamo del: principio del rispetto dei diritti fondamentali, principio di non-discriminazione, principio di qualità e sicurezza, principio di trasparenza e imparzialità, principio del controllo da parte dell'utilizzatore[110]. Vi è poi la appendice I, cui è dedicata la parte più corposa della Carta, che si occupa dello studio approfondito dell'utilizzo dell'intelligenza artificiale nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale per il trattamento delle decisioni e dei dati giudiziari[111]. Seguono altre tre appendici, tra le quali la II si occupa degli utilizzi nei sistemi giudiziari europei, da

[109] Cfr. per il testo in lingua italiana della Carta https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348.

[110] Ivi, p. 3

[111] *Ibidem*.

incoraggiare o da implementare a seguito di ulteriori studi o dopo aver adottato determinate precauzioni. Orbene, ogni disposizione della Carta, e non potrebbe essere altrimenti, risulta orientata al primo principio richiamato nella parte introduttiva: il rispetto dei diritti fondamentali, ossia assicurare che l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali. La Carta richiama espressamente i diritti fondamentali garantiti dalla Convenzione europea dei diritti dell'uomo (CEDU) e dalla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, in particolare le garanzie del diritto di accesso a un giudice e il diritto alla celebrazione di un equo processo, nel rispetto della parità delle armi e del principio del contraddittorio. Viene posta poi l'attenzione sul generale rispetto per i principi dello stato di diritto e dell'indipendenza del giudice nel processo decisionale. La Carta, inoltre, auspica, affinché i principi fondamentali predetti risultino effettivi, fungano da linee guida fin dalle fasi di elaborazione e di apprendimento degli strumenti di intelligenza artificiale[112].

La Carta etica europea sull'utilizzo dell'intelligenza artificiale può definirsi come un coraggioso tentativo di affrontare delle questioni controverse e già attuali sull'utilizzo dell'IA nei sistemi giudiziari europei, nonché un tentativo di evitare di trovarsi impreparati innanzi alle sfide che nel prossimo futuro l'IA presenterà per il settore penale[113]. Al di là della riuscita o meno del tentativo che la CEPEJ ha attuato con la Carta, quindi al di là del pieno recepimento della stessa da parte dei singoli Stati, appare chiaro che l'utilizzo dell'Intelligenza Artificiale in materia penale non possa prescindere dal rispetto dei diritti fondamentali della persona. Dunque, può risultare utile analizzare lo stato dell'arte degli utilizzi dell'IA nel settore della giustizia penale, evidenziando le attuali questioni controverse e le tensioni sussistenti rispetto ai principi fondamentali.

Le questioni che attengono al rapporto tra intelligenza artificiale e giustizia penale, che meritano di essere approfondite, perché suscitano maggiori dubbi alla luce dei di-

[112] Ivi, p. 7.
[113] È da segnalarsi la proposta di regolamento sull'approccio europeo all'Intelligenza Artificiale del 21 aprile 2021 presentata dalla Commissione Europea, volta ad introdurreuna disciplina generale in materia, condivisa da tutti gli stati membri dell'Unione Europea. Anche in questa proposta, che essendo generale va oltre i confini del settore della giustiziapenale, è posto quale obbiettivo principale il rispetto dei diritti fondamentali e dei valorieuropei. Per il testo della proposta di regolamento in lingua inglese https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=EN.

ritti fondamentali della persona, si possono suddividere in quattro macro-aree: la responsabilità penale degli agenti intelligenti; gli strumenti di *law enforcement* (polizia predittiva); l'utilizzo degli algoritmi predittivi per valutare la pericolosità sociale (*risk assessment tools*); la giustizia predittiva (*automated decision systems*)[114].

3. La responsabilità penale degli agenti intelligenti.

La prima questione relativa al rapporto tra intelligenza artificiale e giustizia penale che necessita di essere approfondita riguarda l'opportunità o meno di riconoscere una qualche forma di responsabilità penale per gli agenti intelligenti che commettono reati. Si cerca in altre parole di rispondere alla domanda: *machina delinquere potest*?[115]

Fino a pochi anni fa poteva apparire come una domanda di mero interesse accademico o di interesse fantascientifico, perché poco rispondente alla realtà. Oggi, invece, emerge chiaramente la necessità di fornire una qualche forma di risposta, che possa risolvere una serie di problemi che l'utilizzo così diffuso degli strumenti di IA pone. Si pensi: alle automobili a guida autonoma (*self-driving cars*), che riescono a circolare sulle nostre strade autonomamente, senza alcun controllo umano; agli *high frequency traders* (HFT), strumenti informatici capaci di svolgere migliaia di operazioni al secondo sui mercati finanziari; ai droni che operano negli scenari di guerra quasi in totale autonomia rispetto al controllo umano; alle operazioni chirurgiche delicatissime effettuate in autonomia da macchine intelligenti. Tutte queste attività presentano delle potenzialità "illecite" molto elevate, anche sul versante penalistico. Dunque, la questione è se e quale forma di responsabilità attribuire ad uno strumento di IA che incorra nella commissione di un reato[116].

In primo luogo, è opportuno evidenziare che maggiori difficoltà sorgono in relazione agli strumenti di IA che possono definirsi quasi totalmente autonomi rispetto al controllo umano e quindi imprevedibili. Questa forma di autonomia decisionale è resa possibile dalle tecniche di apprendimento automatico (*machine learning*) o profondo (*deep learning*) che consentono agli strumenti di I.A. di apprendere da sé, sulla base

[114] Cfr. U. RUFFOLO (a cura di), *op. cit*., pp. 531-567.
[115] Domanda mutuata dal contesto che ha portato a riconoscere una forma di responsabilità da reato in capo agli enti con il d.lgs. 231/2001. La domanda ricorrente all'inizio del percorso che poi è culminato nel predetto decreto era infatti *"societas delinquere potest?"* v. DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI (a cura di), *Reati e responsabilità degli enti. Guida al D.Lgs. 8 giugno 2001, n. 231*, II ed., Milano, 2010, pp. 3 ss.
[116] Cfr. F. BASILE, *"Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine"*, in *Diritto Penale e Uomo*, Milano, 2019, pp. 24 ss.

della propria esperienza, quindi di agire successivamente senza alcun intervento umano[117].

Minori problemi sorgono, invece, almeno in linea teorica, rispetto agli agenti intelligenti che possiedono un margine di autonomia limitato rispetto al potere di controllo esercitato dall'essere umano. In queste ipotesi, infatti, sarebbe agevole riconoscere delle forme di responsabilità colpose in capo allo sviluppatore/produttore/utilizzatore, in termini di omesso controllo e/o di omesso impedimento dell'attività criminosa dell'agente intelligente, in base al combinato disposto dell'art. 40 cpv c.p.[118] e delle singole norme che disciplinerebbero gli obblighi legati alle predette posizioni di garanzia. Dunque, l'essere umano assumerebbe, rispetto all'agente intelligente privo di autonomia decisionale, una posizione di garanzia, tutelata da singole norme incriminatrici che obbligherebbero lo sviluppatore/produttore/utilizzatore a impedire la commissione di un reato dell'IA[119].

Se è agevole fornire delle risposte in ordine alla responsabilità da reato degli agenti intelligenti che presentano un margine decisionale limitato, così non è invece per le eventuali responsabilità emergenti nel caso in cui il fatto-reato sia commesso da strumenti di IA che presentano una autonoma capacità decisionale e quindi una intrinseca imprevedibilità. Si fa riferimento a quelle ipotesi nelle quali non si può attribuire una responsabilità in capo allo sviluppatore/produttore/utilizzatore, in quanto l'azione criminosa posta in essere dall'agente intelligente si pone totalmente fuori dalla sfera di controllo e di prevedibilità dell'essere umano. In queste ipotesi, se non si può attribuire la responsabilità penale in capo all'essere umano, in che termini può attribuirsi in capo all'agente intelligente?

Si pongono infatti delle criticità apparentemente insuperabili se facciamo riferimento al tradizionale concetto di responsabilità penale personale e colpevole, orientato alla finalità rieducativa della pena[120], sancito dall'art. 27 della Costituzione (primo e terzo comma)[121]. Innanzitutto, se risulta agevole individuare l'elemento materiale nel fatto-reato dell'agente intelligente autonomo, non risulta invece possibile individuare

---

[117] Cfr. U. RUFFOLO (a cura di), *op. cit.*, p. 533.
[118] *"Non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo"*.
[119] Cfr. http://fornarieassociati.com/focus-ai-artificial-intelligence-la-frontiera-del-diritto/.
[120] Cfr. U. RUFFOLO (a cura di), *op. cit.*, p. 549.
[121] L'art. 27 Cost. recita: <<*La responsabilità penale è personale.*
L'imputato non è considerato colpevole sino alla condanna definitiva.
Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere allarieducazione del condannato.
Non è ammessa la pena di morte>>.

nel comportamento della macchina di IA l'elemento psicologico, nei tradizionali termini di dolo o colpa. Appare infatti complicato individuare in un agente intelligente la coscienza e la volontà di agire, allo stesso modo non si riesce ad immaginare un atteggiamento psicologico dell'IA nei termini di imprudenza, negligenza o imperizia.

Inoltre, nella prospettiva della funzione rieducativa della pena, l'agente di IA: da un lato, nei termini di prevenzione speciale, non può percepire il disvalore del fatto commesso e quindi la pena conseguente come giusta, non può beneficiare della funzione di risocializzazione, né percepire l'effetto deterrente rispetto alla commissione di ulteriori reati in futuro; dall'altro lato, nei termini di prevenzione generale, sicuramente la pena irrogata nei confronti dell'agente intelligente non può suscitare un effetto deterrente nei confronti di altri agenti di IA, né rafforzare in questi ultimi la fiducia nei confronti dell'ordinamento giuridico[122].

Infine, vi è il problema della scelta della sanzione da irrogare, dato che non appaiono idonee per un agente di IA né la pena detentiva, né quella pecuniaria. Sul punto appare suggestiva la teoria che applicherebbe la sanzione dello spegnimento definitivo o temporaneo della macchina (funzione retributiva della pena), in uno alla sottoposizione della macchina intelligente ad un nuovo "autoapprendimento rieducativo" (funzione di prevenzione speciale)[123].

Sono evidenti, quindi, gli ostacoli che si frappongono, sul piano dei principi fondamentali del nostro ordinamento, ad un eventuale riconoscimento di una forma di responsabilità penale in capo all'agente intelligente che delinque[124].

D'altro canto, non appaiono convincenti neppure i parallelismi, operati da alcuni autori, col percorso che ha portato al riconoscimento di una responsabilità da reato degli enti a seguito del D.Lgs. 231/2001, in un settore, quello appunto degli enti, nel quale si era sempre esclusa una forma di responsabilità da reato autonoma per le persone giuridiche. Il parallelismo non appare convincente, in quanto, presupposto indefettibile dell'attribuzione della responsabilità da reato in capo ad un ente, è la commissione del fatto da parte di un agente umano, elemento umano che risulta invece assente nelle ipotesi di reati realizzati da agenti intelligenti autonomi[125].

---

[122] Cfr. per una disamina approfondita sulla funzione della pena S. MOCCIA, *"Il Diritto Penaletra Essere e Valore, Funzione della Pena e Sistematica Teleologica"*, Napoli, Edizioni Scientifiche Italiane, 1992.
[123] Cfr. F. BASILE, *op. cit.*, pp. 31 e 32.
[124] Tra gli autori che ritengono possibile una forma di responsabilità diretta degli agenti intelligenti cfr. U. PAGALLO, "*The Laws of Robots. Crimes, Contracts and Torts"*, Dordrecht, 2013, pp. 50 ss.
[125] Cfr. U. RUFFOLO (a cura di), *op. cit.*, p. 535 e 536.

Pertanto, è chiaro che ai fini di un riconoscimento in capo agli agenti di IA di una forma di responsabilità penale autonoma, bisogna innanzitutto affrontare, e se è possibile risolvere, le notevoli frizioni che si frappongono rispetto alla tutela dei principi fondamentali in materia penale. Potrebbe forse rivelarsi più proficuo sondare, anche per gli agenti intelligenti autonomi, la teoria della responsabilità colposa da reato dell'IA del produttore/programmatore/utilizzatore, già ipotizzata poc'anzi per i reati commessi dagli agenti intelligenti non autonomi, in virtù delle posizioni di garanzia rivestite dai predetti agenti umani. Certamente, non sarebbe una strada agevole da percorrere, perché porrebbe in capo all'agente umano una posizione di garanzia rispetto ai fatti dell'IA molto ampia, forse impossibile da sostenere nelle ipotesi di totale autonomia degli agenti intelligenti. Il riconoscimento in capo ai soggetti umani di una tale forma di responsabilità potrebbe infatti fornire delle tutele in ordine al perseguimento e alla repressione effettiva dei fatti commessi dall'IA, ma ciò potrebbe avvenire a discapito dell'enorme progresso tecnologico e sociale apportato dall'IA, che rallenterebbe a causa della impossibilità da parte degli agenti umani di adempiere gli obblighi sottesi alle suddette posizioni di garanzia[126].

4. Gli strumenti di law enforcement (polizia predittiva).

Un'altra questione problematica, che concerne il rapporto tra IA e giustizia penale, attiene all'utilizzo da parte delle forze di polizia degli strumenti di *law enforcement*, in particolare di polizia predittiva, al fine di prevenire la commissione dei reati o addirittura di intervenire nello stato di flagranza degli stessi. Gli strumenti di polizia predittiva si servono della capacità da parte dell'IA di elaborare una quantità potenzialmente infinita di dati e di porli in correlazione logica attraverso degli algoritmi. Questa capacità computazionale, propria degli algoritmi di IA, permette di cogliere delle connessioni logiche significative nel mare magnum di dati che oramai abbiamo a disposizione in tutti i settori della vita sociale, riuscendo quindi a trarre informazioni che un cervello umano non sarebbe in grado neppure di percepire[127].

Gli strumenti di polizia predittiva possono essere distinti in due categorie: gli strumenti di individuazione delle cosiddette "zone calde" (*hotspots*) e gli strumenti di

[126] *Ibidem.*
[127] Cfr. G. F. ITALIANO, *"Intelligenza artificiale: passato, presente, futuro",* in F. PIZZETTI (a cura di), *"intelligenza artificiale, protezione dei dati personali e regolazione"*, Giappichelli, 2018, p. 222.

crime linking and profiling. I primi, consentono di individuare le aree geografiche a maggior rischio criminale, i secondi invece consentono di prevedere la commissione di reati seguendo le cosiddette serialità criminali di determinati soggetti[128]. Gli strumenti di polizia predittiva, già da anni utilizzati in UK e Stati Uniti, attualmente coadiuvano anche le forze di polizia del nostro paese; infatti, le Questure di Napoli e Milano hanno elaborato dei software di polizia predittiva propri, che si sono poi diffusi nel resto del territorio italiano[129].

Per quanto concerne gli strumenti di individuazione degli hotspots, questi si fondano su algoritmi che analizzano una enorme quantità di dati inerenti a reati già commessi, fornendo delle vere e proprie mappe, dalle quali è possibile ricavare quali sono i luoghi di una città maggiormente a rischio e quali reati sono commessi con maggiore frequenza. Tra gli algoritmi su cui si basano gli strumenti di individuazione degli *hotspots*, vi è il *Risk Terrain Modeling* (RTM), il quale grazie alla suddetta analisi dei dati, consentirebbe di prevedere la commissione di reati di spaccio di stupefacenti in determinate zone della città (*hotsposts*). In particolare, RTM si serve di una serie di parametri di rischio ambientali e spaziali, quindi criminogenetici, quali: la presenza di luminarie funzionanti, la presenza di locali notturni, di fermate di mezzi pubblici, di bancomat, di compro-oro, di scuole. Sulla scorta della mappa così ottenuta, che individua le zone della città più a rischio, possono pertanto essere programmate tutte le attività di polizia, in funzione preventiva[130].

Per quanto riguarda, invece, gli strumenti *crime linking and profiling*, questi si fondano sul concetto di serialità criminale (*near repeat crimes*): ossia, sull'assunto che per alcuni reati, soprattutto per quelli predatori, vi sarebbe una elevata probabilità che il soggetto che ha realizzato il primo reato, nell'arco del mese successivo e con una percentuale di rischio decrescente, ne realizzi un altro della medesima specie, in un luogo circoscritto all'area geografica del reato commesso in precedenza. Per cui gli strumenti di *crime linking*, a differenza degli strumenti di individuazione degli *hotspots*

[128] Cfr. F. BASILE, *op. cit.*, pp. 11 e 12.
[129] In particolare, si fa riferimento ai software *X-Law* (Napoli) e *Keycrime* (Milano). Per quantoriguarda software stranieri, molto citato è *PredPol*, elaborato da alcuni ricercatori della Università della California di Los Angeles, ed attualmente utilizzato in numerosi stati degli Stati Uniti e nel resto del mondo; Cfr. U. RUFFOLO (a cura di), *op. cit*., p. 552.
[130] Cfr. F. BASILE, *op. cit.*, p. 11; J. CAPLAN, L. KENNEDY, J. BARNUM, E. PIZA, *"Crime in context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics Of Criminogenic Behavior Setting"*, in *Journal of Contemporary Criminal Justice*, 2017, pp. 133 ss.

che forniscono una mappa delle aree urbane a rischio (*placed- based system*), individuano dei soggetti, che con elevata probabilità commetteranno ulteriori reati (*person-based system*)[131].

Orbene, gli strumenti di polizia predittiva consentirebbero di prevenire determinati reati (soprattutto sessuali o predatori), o comunque la efficace repressione degli stessi attraverso l'arresto in flagranza. Stando ai dati forniti in relazione all'utilizzo di questi strumenti in alcune città degli Stati Uniti, porterebbero ad una riduzione della criminalità che va dal 20% al 70%, a seconda dei reati presi in considerazione[132].

Dunque, l'utilizzo degli strumenti di *law enforcement* sembrerebbe proficuo in un'ottica di prevenzione della criminalità, ma non si possono ignorare le tensioni che possono sorgerein relazione alla tutela dei diritti fondamentali della persona.

In primo luogo, il trattamento di una quantità enorme di dati personali da parte degli strumenti di polizia predittiva può porre dei problemi con la tutela della privacy di tutti isoggetti interessati. Sul punto può risultare utile richiamare l'art. 16 del D. Lgs. 51/2018(decreto sulla protezione dei dati personali in ambito penale), il quale impone al titolare del trattamento di porre in essere le misure tecniche e organizzative adeguate per garantire la protezione dei dati e per tutelare i diritti degli interessati, anche attraverso la pseudonimizzazione; impone, inoltre, che le misure tecniche e organizzative adottate dal titolare del trattamento, garantiscano che, per impostazione predefinita (*privacy by default*), i predetti dati personali non siano resi accessibili a un numero indefinito di persone[133].

In secondo luogo, con riferimento alla raccolta e alla elaborazione dei dati, non si possono ignorare le criticità che possono sorgere in relazione al principio di uguaglianza (art. 3 Cost.), tenendo conto dei potenziali effetti discriminatori che possono scaturire dall'utilizzo dei suddetti strumenti. In particolare, il potenziale effetto discriminatorio è insito nell'attività di raccolta dei dati, ossia nella scelta dei fattori di rischio da considerare ai fini della mappatura dei rischi (*hotspots*) o della individuazione dei soggetti a rischio (*crime linking and profiling*). Infatti, i fattori di rischio considerati dagli strumenti di polizia predittiva possono riguardare l'età, il genere, l'etnia, il luogo

[131] Cfr. U. RUFFOLO (a cura di), *op. cit*., pp. 540 e 541.
[132] In particolare, si fa riferimento al software *Predpol* utilizzato dal dipartimento di polizia di Los Angeles, i cui dati sono reperibili sul sito: https://www.predpol.com/.
[133] Il testo del decreto è rinvenibile *online* sulla gazzetta ufficiale: https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

di residenza, le condizioni socioeconomiche, le abitudini di vita, anche sessuali o morali, i luoghi e le amicizie frequentati.

Non si può inoltre sottovalutare l'effetto "autoavverante" che può derivare dall'utilizzo di questi strumenti. È chiaro che se il software di polizia predittiva utilizzato, suggerisce di porre maggiore attenzione e/o di allocare maggiori risorse verso determinate aree urbane oppure nei confronti determinati soggetti considerati a rischio, verranno accertati più reati nelle predette aree o più reati commessi dai predetti soggetti, anche se magari i tassi di criminalità reali non sono più elevati della media[134]. La maggiore attenzione prestata dalle forze di polizia verso una determinata area urbana o verso determinati soggetti a rischio, inoltre, potrebbe causare un calo di attenzione e di risorse verso altre aree urbane o soggetti che l'algoritmo non ha saputo individuare, formando delle vere e proprie aree di impunità[135]. Non è, infine, da ignorare che l'utilizzo degli strumenti di polizia predittiva porta inevitabilmente alla "militarizzazione" finalizzata al controllo di determinate aree urbane o al controllo di determinati soggetti, ponendo in qualche modo in secondo piano l'attività necessaria finalizzata alla riduzione dei fattori criminogeni, di tipo sociale o individuale[136].

5. L'utilizzo degli algoritmi predittivi per valutare la pericolosità sociale (risk assessment tools).

La capacità predittiva degli algoritmi utilizzati dai sistemi di IA è propria non solo degli strumenti di *law enforcement* analizzati poc'anzi, ma viene altresì sfruttata dai sistemi di IA di valutazione della pericolosità sociale (*risk assessment tools*). A differenza degli strumenti di polizia predittiva, finalizzati alla prevenzione dei reati attraverso la sorveglianza di determinate aree urbane (*hotspots*) o di soggetti considerati a rischio (*crime linking and profiling*), i sistemi di valutazione della pericolosità sociale svolgono la funzione di prevenzione in una fase successiva, in quanto la predetta valutazione ha ad oggetto il pericolo di commissione di futuri reati di soggetti già sottoposti a procedimento penale[137].

---

[134] Cfr. G. UBERTIS, "Intelligenza Artificiale, Giustizia Penale, Controllo Umano Significativo", pp. 10 e 11, articolo scaricabile dal presente link: http://www.antoniocasella.eu/dnlaw/Ubertis_15ott20.pdf.
[135] Cfr. F. BASILE, *op. cit.*, p. 13.
[136] Cfr. G. UBERTIS, *op. cit.*, p. 11.
[137] Cfr. http://fornarieassociati.com/focus-ai-artificial-intelligence-la-frontiera-del-diritto/.

Orbene, i sistemi di IA di valutazione della pericolosità sociale, così come gli strumenti di polizia predittiva, utilizzano degli algoritmi di *machine learning* in grado di elaborare e porre in correlazione logica una quantità di dati potenzialmente infinita. Tali algoritmi, ai fini della valutazione della pericolosità sociale di un soggetto, seguono un approccio *evidence-based*, riguardando soltanto dati oggettivi, essendo in grado addirittura di sostituire o almeno di supportare le valutazioni del giudice, basate per lo più sul fattore intuitivo[138].

I dati elaborati dagli algoritmi ai fini della valutazione della pericolosità sociale del soggetto presuppongono l'individuazione di una serie di fattori di rischio, i quali possono riguardare: l'etnia, il sesso, l'età, le condizioni sociali ed economiche, i precedenti penali propri o di familiari, le frequentazioni, le abitudini di vita. Ad ognuno dei predetti fattori di rischio, l'algoritmo di IA attribuisce un determinato punteggio (*score*). Dalla combinazione dei punteggi assegnati dall'algoritmo è possibile ricavare il punteggio generale attribuito al soggetto, che misurerà il suo grado di pericolosità sociale[139].

I sistemi di IA di valutazione della pericolosità sociale sono per lo più utilizzati negli Stati Uniti, manca invece un raffronto per quanto riguarda il nostro paese. Oltreoceano, i sistemi di IA di valutazione della pericolosità sociale sono sovente impiegati in diverse fasi del procedimento: nella fase cautelare (*pre-sentencing*), per valutare l'opportunità di liberare, dietro il pagamento di una cauzione (*bail*), il soggetto sottoposto alla custodia cautelare in carcere, quindi in questo caso la valutazione ha ad oggetto il pericolo che la liberazione possa compromettere il processo che sarà celebrato di lì a poco; nella fase decisionale (*sentencing*), per la commisurazione della pena da comminare al soggetto considerato colpevole; nella fase esecutiva, per valutare l'opportunità dell'applicazione di misure alternative alla detenzione (*probation*) o di concedere la liberazione condizionale (*parole*) [140].

L'esperienza statunitense nell'utilizzo di siffatti sistemi consente di fare delle considerazioni in merito alle criticità emerse in relazione alla salvaguardia dei diritti umani fondamentali. Emblematico al riguardo, risulta l'oramai famigerato caso *Loomis*, che prende il nome dall'imputato che aveva fatto ricorso alla Corte Suprema del

[138] Cfr. G. ZARA, *"Tra il probabile e il certo. La valutazione dei rischi di violenza e di recidiva criminale"*, in *Diritto Penale Contemporaneo*, 20 maggio 2016.
[139] L. CASTELLETTI, G. RIVELLINI, E. STRATICÒ, *"Efficacia predittiva degli strumenti di Violence Risk assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana"*, in *Journal of Psychopatology*, 2014, pp. 153 ss.
[140] Cfr. http://fornarieassociati.com/focus-ai-artificial-intelligence-la-frontiera-del-diritto/.

Winsconsin, contestando la pena eccessiva (senza neppure *parole*) comminata dalla corte locale, la quale in sede di *sentencing* con l'ausilio del software COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) aveva valutato l'imputato come soggetto ad alto rischio di recidiva. In particolare, l'imputato ricorrente, contestava che il software utilizzato dalla corte locale fondava le valutazioni sulla pericolosità sociale su pregiudizi razziali. Inoltre, veniva contestata la mancanza di trasparenza inerente al meccanismo di funzionamento del software e quindi l'impossibilità di esercitare compiutamente il diritto di difesa. Tuttavia, la Corte del Winsconsin confermò la legittimità della decisione assunta dalla corte di grado inferiore, sostenendo che i giudici locali avevano utilizzato il software COMPAS come mero strumento di ausilio, le cui valutazioni erano state sottoposte al vaglio umano e raffrontate a tutti gli altri elementi emersi nel corso del processo[141].

A dispetto della decisione della Corte del Winsconsin, le tesi sostenute dai ricorrenti nel caso *Loomis* non sembrerebbero prive di fondamento: in particolare, un gruppo di ricercatori nel 2016 ha pubblicato uno studio che confermerebbe i pregiudizi razziali insiti nell'algoritmo utilizzato da COMPAS, il quale sovrastimerebbe il rischio di recidiva delle persone di colore e sottostimerebbe invece lo stesso rischio per gli imputati bianchi[142].

Al netto della decisione della Corte del Winsconsin, il caso *Loomis* sembra però aver sancito, almeno, il principio che il giudice non possa recepire acriticamente i risultati forniti dal software, in quanto vi è "necessità che l'organo giudicante applichi i risultati del programma facendo esercizio della propria discrezionalità sulla base del bilanciamento con altri fattori"[143]. Tale assunto, può certamente trovare una corrispondenza con quanto statuito dagli art. 22 reg. n. 2016/679, 11 dir. n. 2016/680/UE e 8 d.lgs. n. 51 del 2018 in materia di privacy. Queste norme, infatti, vietano le decisioni giurisdizionali basate esclusivamente su trattamenti automatizzati, imponendo al giudicante di valutare i risultati elaborati dai software di IA alla stregua di meri indizi, i

[141] Cfr. E. ISTRIANI, *"Algorithmic Due Process: Mistaken Accountability and Attribution in State v.Loomis"*, in *Harvard JOLT Digest*, 2017.
[142] Si fa riferimento allo studio commissionato dalla Organizzazione Non Governativa *ProPublica* basato su un campione di 7.000 persone della Florida giudicate con l'ausilio del software COMPAS, Cfr. J. ANGWIN, J. LARSON, S. MATTU, L. KIRCHNER, *"Machine Bias"*, in www.propublica.org, 2016.
[143] Cfr. C. PARODI, V. SELLAROLI, *"Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco"*, in *Diritto Penale Contemporaneo*, 2019, n. 6, pp. 69 e 70.

quali devono necessariamente ottenere riscontro attraverso ulteriori elementi di prova[144].

Orbene, è chiaro che l'utilizzo di algoritmi predittivi per la valutazione della pericolosità sociale potrebbe porsi in contrasto con i principi fondamentali in materia penale.

In primo luogo, si rilevano tensioni con il principio di uguaglianza (art. 3 Cost.), essendo gli algoritmi di IA ontologicamente antiegualitari, prendendo in considerazione soltanto determinati elementi anziché altri (etnia, sesso, età, condizioni sociali ed economiche, precedenti penali *etc*…)[145].

In secondo luogo, nonostante, come dianzi analizzato, in Europa e nel nostro paese vi siano interventi legislativi recenti che vietano le decisioni giurisdizionali basate esclusivamente sul trattamento automatizzato dei dati personali, permangono le criticità legate al principio di trasparenza relativo ai processi computazionali degli algoritmi e di riflesso quindi criticità legate al diritto di difesa ex artt. 24 e 111 Cost., segnatamente ai principi di parità delle armi, del contraddittorio nella formazione della prova e al principio di motivazione dei provvedimenti giurisdizionali. In sostanza, nonostante vi siano disposizioni che sanciscano che i software predittivi possano essere utilizzati soltanto come strumenti di mero ausilio dal giudicante, permane l'imperscrutabilità del processo che porta il software ad una determinata valutazione (ad es. quella riguardante la pericolosità sociale), quindi l'impossibilità di apprestare una strategia difensiva atta a contestare la legittimità del processo valutativo[146].

In ultimo, non è da sottovalutare l'ulteriore rischio, insito nella standardizzazione delle informazioni derivante dall'utilizzo degli algoritmi predittivi, che si prediliga un "diritto penale d'autore", a discapito di un "diritto penale del fatto", così come invece sancito dall'art. 25, comma 2, della Costituzione[147].

6. La giustizia predittiva (automated decision systems).

Per quanto riguarda gli algoritmi predittivi, si prospetta un loro utilizzo, in sede giudiziale, anche con riferimento al momento formativo della decisione/sentenza. Gli strumenti di IA di giustizia predittiva avrebbero potenzialmente la capacità di sostituire

[144] Cfr. M. GIALUZ, "*Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei riskassessment tools tra Stati Uniti ed Europa"*, in *Diritto Penale Contemporaneo*, 2019, p. 17.
[145] Cfr. U. RUFFOLO (a cura di), *op. cit.*, p. 557.
[146] *Ivi*, p. 560.
[147] *Ibidem*, p. 559.

totalmente il giudicante nella fase decisionale, sulla scorta di una valutazione autonoma delle prove raccolte in giudizio, promettendo non solo di ridurre gli errori giudiziari ma anche di operare una più adeguata commisurazione delle pene. Le predette operazioni sarebbero rese possibili dalla infinita quantità di dati che gli algoritmi di IA sono capaci di elaborare, attingendo dalle banche-dati giurisprudenziali e legislative[148].

L'utilizzo degli strumenti di giustizia predittiva si è sviluppato soprattutto negli Stati Uniti e principalmente in ambito civilistico (in materia di risarcimento danni, assicurazioni, danni da prodotto)[149]. Non è inoltre da sottovalutare, nello stesso settore, l'utilizzo diffuso degli algoritmi predittivi per l'applicazione di metodi alternativi di risoluzione delle controversie[150].

Orbene, la potenziale estensione dell'utilizzo di tali algoritmi, alla fase decisionale del processo penale, desta oggi notevoli preoccupazioni tra gli studiosi e gli operatori del diritto. Emblematico al riguardo è quanto statuito nella Carta etica europea per l'uso dell'intelligenza artificiale adottata dalla Commissione per l'efficacia della giustizia (CEPEJ) del Consiglio d'Europa. Infatti, tra i principi che assurgono a linee guida della Carta, oltre al principio del rispetto dei diritti fondamentali su cui già ci siamo soffermati, pare opportuno richiamare il principio di garanzia del controllo umano. Tale principio, assume una notevole importanza in relazione alle potenziali criticità che possono scaturire dall'utilizzo degli algoritmi predittivi in sede decisionale. Avrebbe, infatti, la finalità di evitare che le decisioni del giudice penale si possano basare esclusivamente sui risultati forniti dagli strumenti di IA, in assenza quindi di valutazioni umane sugli stessi e quindi anche di riscontri con altri elementi emersi in sede istruttoria[151].

Le criticità che possono emergere in relazione all'utilizzo degli strumenti di giustizia predittiva non riguardano soltanto il principio di garanzia del controllo umano, bensì anche e soprattutto il rispetto dei diritti fondamentali della persona. Infatti, come già visto per gli altri strumenti di IA che sfruttano le capacità computazionali degli algoritmi, si pongono notevoli perplessità in riferimento ai potenziali pregiudizi, razziali

---

[148] Cfr. U. RUFFOLO (a cura di), *op. cit.*, pp. 553 e 554.
[149] Cfr. J. NIEVA FENOLL, *Inteligencia artificial y proceso giudicial*, 2018, trad. in italiano di P.COMOGLIO, *Intelligenza artificiale e processo*, Giappichelli, 2019.
[150] Cfr. F. BASILE, *op. cit.*, p. 14.
[151] Cfr. Testo della carta reperibile qui https://rm.coe.int/carta-etica-europea-sull-utilizzo- dell-intelligenza-artificiale-nei-si/1680993348.

ma non solo, che possono condizionare le elaborazioni fornite dagli strumenti. Si rilevano pertanto delle tensioni in relazione al principio di uguaglianza (art. 3 Cost.), in quanto gli algoritmi risultano geneticamente antiegualitari, attingendo necessariamente soltanto dalle informazioni di cui dispongono in quel momento e non da altre[152].

L'utilizzo degli strumenti di giustizia predittiva pone inoltre delle tensioni nella prospettiva dei principi del "giusto processo" (art. 111 Cost.) e del diritto di difesa (art. 24 Cost.). L'impossibilità di sondare i meccanismi tecnici che governano il funzionamento del singolo strumento di IA, sulla scorta dell'esigenza di tutela del segreto commerciale dei software utilizzati, rende di fatto insondabile la motivazione a suffragio della decisione adottata. Dunque, il rischio è che manchi una motivazione o che la decisione adottata dal giudice sia basata su una motivazione soltanto apparente (*black box decision*), rendendo quindi estremamente difficoltoso l'esercizio del diritto di difesa, in particolare la contestazione e il vaglio degli elementi fondativi della decisione[153].

D'altro canto, c'è da rilevare che il mezzo di prova principe del processo penale è la testimonianza, ed è difficile immaginare una valutazione puntuale del sistema di IA inerente alla veridicità o meno del soggetto audito; in particolare, poi, nei processi indiziari l'algoritmo predittivo dovrebbe stabilire se gli indizi possano essere considerati "gravi, precisi e concordanti" (art. 192, comma 2, c.p.p.). Infine, il sistema di IA dovrebbe valutare se il compendio probatorio emerso nel corso dell'istruttoria dibattimentale possa fondare una decisione di colpevolezza sulla scorta del canone dell'"oltre ogni ragionevole dubbio" (art. 533, comma 1, c.p.p.). L'applicazione di questo canone appare in contrasto col meccanismo di funzionamento degli algoritmi di IA, capaci al più di fornire risposte secondo logiche binarie (sì/no, vero/falso) o probabilistiche (sì al 65%, vero al 50%)[154].

7. Riflessioni conclusive.

Come si è avuto modo di constatare, l'intelligenza artificiale è presente in tutti gli ambiti della nostra vita e continuerà ad esserlo sempre di più nei prossimi anni.

---

[152] Cfr. U. RUFFOLO (a cura di), *op. cit.*, p. 557.
[153] Cfr. S. QUATTROCOLO, *"Equità del processo penale e automated evidence alla luce della giurisprudenza della Corte europea dei diritti dell'uomo",* in *Rev. Italo-Espanola Der. Proc.*, vol. 2/2019, in ptc. 11, 13.
[154] Cfr. F. BASILE, *op. cit.*, pp. 15 e 16.

Nella maggior parte dei casi, l'apporto fornito dalle tecnologie di IA risulta positivo, in termini di rapporto costi sociali/benefici, anche se non sono pochi gli ambiti in cui emergono delle criticità. Le criticità che emergono a fronte dell'utilizzo dei sistemi di IA richiedono riflessioni approfondite, ricerche e studi scientifici, infine, norme giuridiche finalizzate alla regolamentazione dei settori in cui i sistemi vanno ad operare. Infatti, le riflessioni che animano i dibattiti sull'utilizzo dell'IA, spesso, alimentano ricerche e studi, i quali vanno ad arricchire le discussioni che si tengono nell'ambito dei consessi istituzionali, chiamati ad assumere decisioni e ad adottare norme.

Tutti questi passaggi richiedono del tempo, a causa della complessità delle questioni che di volta in volta emergono, e ciò deve essere raffrontato alla velocità di sviluppo delle tecnologie di IA. Soprattutto se guardiamo da una prospettiva europea, entrano in gioco anche degli interessi economici molto rilevanti, se si considera che i nostri *competitors* globali(Stati Uniti e Cina) sono in una fase molto avanzata per quanto riguarda la ricerca, l'implementazione dei sistemi di IA e le relative legislazioni a supporto.

Per quanto riguarda il settore della giustizia penale, nel nostro paese, finora, strumenti di IA sono adoperati soltanto nel settore delle indagini di polizia (*law enforcement*), a differenza invece di quanto accade negli Stati Uniti, ove già da tempo hanno implementato l'utilizzo di software che sfruttano algoritmi predittivi in sede decisionale, per l'accertamento della responsabilità penale (*automated decision systems*), o in più fasi del procedimento, ai fini della valutazione della pericolosità sociale (*risk assessment tools*).

Ciò che avviene negli Stati Uniti potrebbe probabilmente accadere in Europa e nel nostro paese nei prossimi anni, anche se i legislatori sovranazionali, così come quello interno, appaiono più cauti, data la particolare attenzione rivolta alle criticità rilevate in relazione ai diritti fondamentali della persona.

D'altro canto, non si può ignorare che le difficoltà nell'adottare una disciplina puntuale in materia di IA, pongono indirettamente un freno dal punto di vista della crescita economica.

La carta etica sull'utilizzo dell'intelligenza artificiale, gli ultimi interventi in materia di privacy, nonché la proposta di regolamento della Commissione Europea sull'approccio europeo all'intelligenza artificiale, forniscono un quadro giuridico e

delle linee guida entro cui i legislatori dei singoli stati europei devono operare, assumendo però quale vincolo fondante i diritti fondamentali della persona in materia penale sanciti dalla CEDU e in ambito UE.

È auspicabile quindi che si intervenga con una disciplina organica in materia di IA, al fine di intercettare e cavalcare gli sviluppi sociali ed economici positivi apportati dal progresso tecnologico. Allo stesso modo, si attendono degli interventi nel settore della giustizia penale, almeno al fine di regolamentare gli utilizzi di IA già presenti (*law enforcement*).

È chiaro però che bisognerà tener conto che il progresso sociale, economico e tecnologico non possono avanzare a discapito dei principi fondamentali su cui si fondano i nostri ordinamenti.

I TRATTAMENTI DI DATI CHE FANNO USO DI NUOVE TECNOLOGIE E LA PRESUNZIONE DI ELEVATA RISCHIOSITÀ PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE: DPIA E INCERTEZZE APPLICATIVE

di Sara Sestito

SOMMARIO: 1. Cos'è la DPIA e quali sono i trattamenti che la richiedono – 2. La vaghezza del legislatore – 3. La redazione della DPIA e la sua flessibilità. – 4. Note Bibliografiche.

Abstract: *Il Regolamento EU 2016/679 in materia di protezione dei dati personali, in particolare all'articolo 35, qualifica come fattispecie ad alto rischio i trattamenti di dati che fanno uso di "nuove tecnologie" e in tali casi impone all'autore del trattamento di effettuare una valutazione del potenziale impatto che esso genera sui diritti e le libertà degli interessati affinché possano essere individuate le misure opportune atte ad escluderlo o mitigarlo. Questo lavoro mette principalmente in luce la vaghezza del legislatore in merito che seppur da un lato offre flessibilità all'interprete dall'altro suscita incertezze e si propone, inoltre, di sottolineare l'importanza della DPIA quale adempimento dinamico.*

1. Cos'è la DPIA e quali sono i trattamenti che la richiedono

Per evitare il prodursi di effetti dannosi sui diritti e le libertà delle persone fisiche in occasione di un trattamento dei dati che prevede l'uso di "nuove tecnologie", l'articolo 35 del Regolamento EU 2016/679 in materia di trattamento dei dati personali richiede all'autore del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment o DPIA secondo il suo acronimo inglese). Si tratta di un'operazione che si qualifica come parte integrante dell'approccio proattivo dal Regolamento[155] e, più nello specifico, di un onere posto a carico di chi elabora i dati che, prima che il trattamento abbia luogo, effettua un'analisi dell'impatto che questo produce sulla protezione dei dati, ossia valuta i rischi a cui sono espo-

[155] A. MORETTI, *Intelligenza artificiale: data protection per una governance condivisa*, in Giustizia civile, in *giustiziacivile.com*, 2020, 9 ss.

sti gli interessati e individua le misure opportune per limitarli e contenerli (Considerando n. 84). In particolare, la DPIA ha lo scopo di individuare la "probabilità" e la "gravità" di una violazione dei diritti e delle libertà degli interessati che deriva dal trattamento (Considerando n. 76).

La valutazione del rischio non è richiesta per qualunque tipo di trattamento ma risulta obbligatoria solo nell'ipotesi in cui il trattamento è "suscettibile di causare un rischio elevato per i diritti e le libertà delle persone fisiche" tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso[156]. L'articolo 35 prevede una sorta di presunzione di elevata rischiosità dei trattamenti che fanno uso di "nuove tecnologie" e il ricorso alla DPIA ha, dunque, lo scopo di stimare e controllare l'impatto dell'uso di strumenti innovativi e non ancora adeguatamente conosciuti sulla protezione dei dati[157].

2. La vaghezza del legislatore

Al riguardo, si lamenta la vaghezza del dettato normativo, in primo luogo del riferimento alle "nuove tecnologie", in quanto categoria a-tecnica e potenzialmente molto estesa e variabile[158].

Altrettanta indeterminatezza deriva dai tre specifici casi menzionati all'articolo 35 par. 3 in cui opera una sorta di presunzione di rischio (casi che, tuttavia, non rappresentano un elenco esaustivo poiché l'analisi dei potenziali rischi che un trattamento dei dati comporta può essere effettuata anche in casi diversi[159]). Segnatamente, la norma qualifica come fattispecie ad alto rischio a) i trattamenti che comportino una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano

---

[156] ARTICLE 29 WORKING PARTY, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 ottobre 2017, 5. Al contrario, la DPIA non sarà obbligatoria quando: "*il trattamento non è tale da presentare un rischio elevato; la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati […]; le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate; un trattamento, ex art. 6, par. 1, lett. c) o e), trovi una base giuridica nel diritto dell'Unione o dello Stato membro, (art. 35, par. 10) a meno che uno Stato membro non abbia dichiarato che la DPIA sia necessaria; il trattamento sia incluso nell'elenco facoltativo delle tipologie di trattamento ex art. 35, par. 5)*", 14 ss.

[157] F. CECAMORE, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, in *GDPR e Normativa Privacy Commentario*, (a cura) G. M. Riccio, G. Scorza, E. Belisario, Milano, 2018, 322 ss.

[158] F. CECAMORE, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, *op. cit*.

[159] F. CECAMORE, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, *op. cit*.

decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico": anche in questi casi si fa riferimento a concetti molto ampi tra cui quello di "valutazione sistematica e globale", di "[effetti che] incidono in modo analogo significativamente su dette persone fisiche" e di "larga scala" che, seppur da un lato offrono flessibilità all'interprete, dall'altro comportano incertezze[160].

La poca chiarezza del legislatore non sembra essere compensata neppure dalle indicazioni fornite dai Considerando. Ne è un esempio il Considerando n. 91 che identifica come trattamenti su larga scala quelli che "mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati" ed aggiunge che "il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati". Anche in questi casi la terminologia impiegata provoca un elevato grado di incertezza che deriva, nello specifico, sia dall'uso dei condizionali, sia da alcune potenziali incongruenze nei parametri o negli esempi forniti. Ad esempio, si tratta di capire come sia possibile individuare un "livello regionale, nazionale o sovranazionale" nei contesti delle reti globali di comunicazione e nel caso di servizi di *cloud computing* e se davvero nel confronto fra un presidio medico di una piccola località con un singolo medico di una grande città con molti pazienti è il primo a dar vita ad un trattamento su larga scala e non il secondo[161]. Plausibilmente, una vera e coerente risposta alle incertezze applicative potrà solamente giungere con il tempo, sia attraverso gli interventi della giurisprudenza, sia grazie al progressivi affacciarsi sulla scena professionale di una classe qualificata di esperti in trattamento[162].

[160] A. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, 2018, 293 ss.
[161] A. MANTELERO, *La gestione del rischio, op. cit*.
[162] A. MANTELERO, *La gestione del rischio, op. cit*.

Ipotesi aggiuntive rispetto a quelle di cui all'articolo 35, par. 3 che sono indice della probabile presenza di rischi elevati e che rendono necessaria una DPIA sono indicate dall'Article 29 Working Party[163]. Si tratta, precisamente, di criteri non obbligatori ma che "possono essere considerati" la cui considerazione è prerogativa delle autorità nazionali, chiaramente in aggiunta dei casi previsti dal Regolamento. Nello specifico, il Gruppo di lavoro ritiene che un trattamento è ad alto rischio quando lo stesso è caratterizzato da:

- l'attribuzione all'interessato, anche tramite sistemi di profilazione, di un "punteggio" ossia di una valutazione o di una misurazione indicata per punti riguardanti aspetti come "il rendimento sul lavoro dell'interessato, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o i movimenti";
- il ricorso a un processo decisionale automatizzato che produca un effetto giuridico o che incida significativamente in modo analogo sul singolo poiché da esso può derivare "l'esclusione o la discriminazione delle persone", dunque fa riferimento all'oggetto dell'articolo 22;
- il monitoraggio sistematico degli interessati qualora "i dati personali siano raccolti in circostanze in cui gli interessati non sono a conoscenza di chi li sta raccogliendo e non sono consapevoli di come saranno utilizzati";
- l'utilizzo di dati sensibili o aventi carattere altamente personale perché l'utilizzo di informazioni che rientrano in tali categorie "aumenta il rischio per i diritti e le libertà degli individui";
- il trattamento di dati "su larga scala" rispetto a cui non viene data una definizione ma il Gruppo di lavoro prende in considerazione al riguardo il numero di persone interessate, il volume dei dati elaborati, la durata dell'attività di elaborazione dei dati e l'estensione geografica dell'attività di trattamento;
- la creazione di corrispondenze o combinazione di insieme di dati ad esempio "provenienti da due o più trattamenti eseguiti per scopi diversi e/o da diversi

[163] L'Article 29 Working Party era un gruppo di lavoro europeo indipendente composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione che il 25 maggio 2018 fu sostituito con il Comitato europeo per la protezione dei dati (EDPB) a seguito dell'entrata in vigore dell'attuale Regolamento europeo 2016/679 in materia di protezione dei dati personali. I principali compiti del Gruppo di lavoro erano quelli di fornire delle linee guida e raccomandazioni agli Stati in merito alla protezione dei dati personali e di promuovere l'omogena applicazione della precedente Direttiva in materia.

responsabili del trattamento secondo modalità che vanno oltre le ragionevoli aspettative dell'interessato";

- l'utilizzo di dati relativi a interessati vulnerabili perché "causa un maggiore squilibrio di potere tra le persone interessate e il responsabile del trattamento, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente, o di opporsi, al trattamento dei loro dati, o di esercitare i loro diritti";
- l'uso innovativo o l'applicazione di nuove soluzioni tecnologiche od organizzative perché possono comportare "nuove forme di raccolta e utilizzo dei dati, ad esempio alcune applicazioni Internet of Things […] potrebbero avere un impatto significativo sulla vita quotidiana degli individui e sulla privacy";
- l'ipotesi in cui il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto; è il caso, ad esempio, di una banca che analizza i dati raccolti sui clienti al fine di decidere se concedere loro un prestito. Anche in questo caso il richiamo immediato è alle situazioni regolate dall'articolo 22[164].

È opportuno precisare che il verificarsi di una di queste ipotesi non comporta automaticamente l'obbligo di effettuare una valutazione d'impatto, tuttavia il realizzarsi di due o più criteri accresce la probabilità che una tale valutazione sia necessaria[165]. Non a caso si è parlato in proposito di una "regola del due" per indicare il fatto che un trattamento può essere caratterizzato da rischio elevato quando si manifestano in concreto almeno due delle situazioni considerate "sintomatiche"[166].

Quando un'attività di trattamento corrisponde ai casi sopra menzionati ma è considerata dal responsabile del trattamento come non "suscettibile di comportare un rischio elevato", il responsabile del trattamento deve giustificare e documentare le ragioni per non effettuare una DPIA. Invece, in caso di dubbio del titolare circa la necessità di procedere alla DPIA, l'Article 29 Working Party precisa che è comunque opportuno effettuarla.

---

[164] ARTICLE 29 WORKING PARTY, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 ottobre 2017, 8 ss.

[165] ARTICLE 29 WORKING PARTY, cit.

[166] G. GALLUS, M. PINTUS, *Data protection impact assessment*, in *Il processo di adeguamento al GDPR. Aggiornato al d.lgs. 10 agosto 2018 n. 101*, (a cura) G. Cassano, V. Colarocco, G. Gallus, F. P. Micozzi, Milano, 2018, 202.

Peraltro, i nove criteri indicati dal Gruppo di lavoro sono stati ripresi dal Garante per la Protezione dei dati personali, quale Autorità nazionale competente, che ha adottato in data 11/10/2018 un elenco di attività di trattamento considerate ad alto rischio, in adempimento del par. 4 dell'articolo 35 che prescrive che le Autorità di controllo redigano un elenco pubblico indicante le tipologie di trattamenti soggetti all'obbligo di DPIA che deve essere poi comunicato al Comitato europeo per la protezione dei dati.

Ulteriore interrogativo è se la sola valutazione dell'impatto che il trattamento dei dati ha sui diritti dell'individuo colga appieno le conseguenze derivanti dal trattamento e se non si debba forse arricchire il suo campo d'indagine[167]. Detto altrimenti, si tratta di capire se si possa adottare una valutazione che colga tutte le criticità connesse all'IA e che, oltre alle conseguenze sui diritti individuali, esamini anche l'impatto sociale, collettivo ed etico dell'elaborazione dei dati[168]. Invero, la protezione fornita dall'articolo 35 sembra già essere di natura collettiva[169]. Secondo le linee guida dell'Article 29 Working Party, infatti, la valutazione d'impatto può coinvolgere anche categorie di soggetti e il paragrafo 9 dell'articolo 35 prevede proprio che, se del caso, il titolare del trattamento raccoglie non solo il parere degli interessati ma anche dei loro rappresentanti (come, ad esempio, i rappresentanti del personale nel caso in cui le attività di profilazione riguardino i dipendenti di un'azienda)[170]. È, tuttavia, difficile prevedere come la norma sarà in concreto applicata poiché può essere soggetta a interpretazioni diverse a seconda del grado di protezione e dell'importanza che si vuole dare alla tutela dei gruppi[171].

Infine, un'altra questione poco chiara è se la valutazione d'impatto debba considerare solo i rischi a cui sono sottoposti i soggetti i cui dati vengono trattati direttamente o se non possano considerarsi anche gli effetti che subiscono gruppi di persone le cui informazioni non siano state direttamente sottoposte a trattamento[172]. Invero, il Gruppo di lavoro sembra escludere quest'ultima ipotesi e pare, invece, riferirsi all'analisi di un potenziale impatto diretto e attuale perché menziona dei rischi strettamente

[167] A. MORETTI, *Intelligenza artificiale: data protection per una governance condivisa*, *op. cit.*
[168] In tal senso, A. MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security review*, 2018, 764 ss.
[169] A. FONDRIESCHI, *A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorithmic Data Processing under the GDPR*, in *Osservatorio del diritto civile e commerciale*, 2019, 456 ss.
[170] ARTICLE 29 WORKING PARTY, cit., 14.
[171] A. FONDRIESCHI, *A Fragile Right*, *op. cit.*
[172] A. FONDRIESCHI, *A Fragile Right*, *op. cit.*

connessi al trattamento dei dati[173]. Tuttavia, le Linee guida fornite per altri argomenti permettono di estendere l'applicazione dell'articolo 35 anche ai casi in cui la produzione di un rischio è solo indiretta. Segnatamente ciò si deduce dalle linee guida rese in tema di decisioni automatizzate di cui all'articolo 22 poiché affermano che "effetti negativi sulla persona potrebbero riguardare anche soggetti diversi da quello a cui si riferisce la decisione automatizzata"[174]. A tal proposito, l'esempio richiamato dal Gruppo di lavoro è quello di una società di carte di credito che assume la decisione di ridurre i limiti di carta di un cliente non in base ai suoi precedenti pagamenti ma in base ai dati relativi ad altri clienti che vivono nella sua stessa zona e fanno acquisti negli stessi negozi[175]. Inoltre, lo stesso articolo 35 prevede che venga svolta una valutazione del rischio in occasione della raccolta di dati su "larga scala" che permette probabilmente di prendere in considerazione anche i casi in cui il rischio è solo potenziale e si ripercuote anche sui soggetti non direttamente coinvolti in attività di trattamento[176]. Questo è il caso, ad esempio, del trattamento su larga scala dei dati sanitari dei pazienti di un grande ospedale al fine di prevedere la possibilità di sviluppare una determinata malattia: questo tipo di trattamento può avere notevoli ripercussioni anche su soggetti con caratteristiche simili a quelle dei pazienti a cui i dati si riferiscono seppure i loro dati non siano stati direttamente elaborati[177].

3. La redazione della DPIA e la sua flessibilità

Rispetto alla redazione della valutazione d'impatto, il Regolamento non prevede forme vincolate e può, dunque, essere scelta in base alle esigenze concrete di chi tratta i dati. Dunque, ad esempio, il titolare del trattamento di piccole dimensioni potrà progettare e attuare una valutazione d'impatto adatta alla propria organizzazione[178]. L'Article 29 Working Party comunque incoraggia lo sviluppo di modalità di valutazione d'impatto specifiche dei vari settori[179].

Riguardo al procedimento della DPIA, questo può essere suddiviso in più momenti. Nello specifico, si ravvisa una prima fase di analisi del trattamento in cui il

[173] ARTICLE 29 WORKING PARTY, cit., 22.
[174] ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018, 22.
[175] ARTICLE 29 WORKING PARTY, cit.
[176] A. FONDRIESCHI, *A Fragile Right*, *op. cit*.
[177] A. FONDRIESCHI, *A Fragile Right*, *op. cit*.
[178] ARTICLE 29 WORKING PARTY, cit., 20.
[179] ARTICLE 29 WORKING PARTY, cit., 20 ss.

titolare descrive in modo completo, coerente, chiaro e non generico il trattamento[180], le sue finalità e valuta la necessità e la proporzionalità dell'elaborazione dei dati rispetto agli scopi[181]; una seconda fase di valutazione dei rischi per i diritti degli interessati e una fase ulteriore di definizione delle misure idonee ad escludere o mitigare tale rischio[182]. A queste fasi faranno poi seguito quelle di verifica dell'efficienza delle misure adottate e di aggiornamento periodico della valutazione, quest'ultima solo eventuale, che garantiscono l'efficacia della DPIA. Poiché per mantenere alto il livello di protezione degli interessati può essere effettuato nuovamente l'esame del rischio, quello della DPIA è, dunque, un "adempimento dinamico". Il par. 11 dell'articolo 35 prevede, più nello specifico, che la stima dell'impatto del trattamento dovrà essere ripetuta con cadenza periodica e ogniqualvolta sia necessario, vale a dire quando insorgano variazioni del rischio. La flessibilità della DPIA è una caratteristica che ben si adatta all'ambiente dei dati che facilmente muta nel tempo[183]: non è difficile, infatti, che il trattamento subisca delle variazioni, ad esempio qualora si raccolgano dati diversi o quando a seguito di nuove modalità di attenuazione del rischio questo si riduce e rende la DPIA non più necessaria[184]. Pertanto, risulta necessario che la stima del rischio si concentri non tanto sullo scopo del trattamento determinato al momento della raccolta dei dati, quanto su quello desumibile dall'utilizzo in concreto dei dati e dall'evolversi del trattamento[185].

4. Note Bibliografiche

ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018.

ARTICLE 29 WORKING PARTY, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 2017.

[180] F. CECAMORE, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, *op. cit.*, 327.
[181] A. MANTELERO, Il nuovo approccio, op. cit., 311.
[182] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Milano, 2018, 316 ss.
[183] E. BATTELLI, G. D'IPPOLITO, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, in *Commentario del codice civile* diretto da E. Gabrielli, (a cura) A. Barba, S. Pagliantini, Milano, 2019, 675.
[184] E. BATTELLI, G. D'IPPOLITO, *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, *op. cit*.
[185] A. MANTELERO, *Il nuovo approccio*, *op. cit*., 312.

BATTELLI E., D'IPPOLITO G., *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, in *Commentario del codice civile* diretto da E. Gabrielli, (a cura) A. Barba, S. Pagliantini, Milano, 2019, 675.

CECAMORE F., *Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*, in *GDPR e Normativa Privacy Commentario*, (a cura) G. M. Riccio, G. Scorza, E. Belisario, Milano, 2018, 322 ss.

FONDRIESCHI A., *A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorithmic Data Processing under the GDPR*, in *Osservatorio del diritto civile e commerciale*, 2019, 456 ss.

GALLUS G., PINTUS M., *Data protection impact assessment*, in *Il processo di adeguamento al GDPR. Aggiornato al d.lgs. 10 agosto 2018 n. 101*, (a cura) G. Cassano, V. Colarocco, G. Gallus, F. P. Micozzi, Milano, 2018, 202.

MANTELERO A., *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security review*, 2018, 764 ss.

MANTELERO A., *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, 2018, 293 ss.

MORETTI A., *Intelligenza artificiale: data protection per una governance condivisa*, in Giustizia civile, in *giustiziacivile.com*, 2020, 9 ss.

SOFFIENTINI M., *Privacy. Protezione e trattamento dei dati*, Milano, 2018.

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it