Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Daniele Imbruglia nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (https://web.uniroma1.it/deap/ogid - jodi.deap@uniroma1.it).

* Contributo non sottoposto a referaggio ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

1. L'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (D.Lgs. 8 novembre 2021, n. 177).

Il 12 dicembre 2021 è entrato in vigore il Decreto Legislativo 177/2021 del 5 novembre 2021 (il "**Decreto**"), attuativo della Direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (la "**Direttiva**"). Il Decreto (emanato dopo il termine prescritto dal legislatore europeo del 7 giugno 2021) è frutto dell'ampia delega conferita al Governo ai fini del recepimento della Direttiva all'interno della legislazione nazionale.

L'obiettivo dichiarato della Direttiva - e dunque del D.Lgs. di adeguamento - è quello di adattare gli strumenti di tutela del diritto d'autore alla modernizzazione generata dall'evoluzione tecnologica ed in particolare da nuove forme di comunicazione, caricamento, condivisione e creazione dei contenuti, le quali costituiscono inedite modalità di riproduzione e "moltiplicazione" dell'opera protetta, che potenzialmente minano l'armonizzazione del diritto d'autore tra gli Stati membri.

In particolare, le disposizioni della Direttiva concernono: l'adeguamento di talune eccezioni e limitazioni all'ambiente digitale e al contesto transfrontaliero (Titolo II); misure volte a facilitare le procedure di concessione delle licenze e a garantire un più ampio accesso ai contenuti (Titolo III), facilitando in particolare, ma non solo, la divulgazione delle opere fuori commercio (Capo I), la concessione di licenze collettive con effetto esteso (Capo II), l'accesso e disponibilità di opere audiovisive su piattaforme di video su richiesta (Capo III), la previsione concernente le opere delle arti visive di dominio pubblico (Capo IV); misure miranti a garantire il buon funzionamento del mercato per il diritto d'autore (Titolo IV), segnatamente la protezione delle pubblicazioni giornalistiche in caso di utilizzo *online* (Capo I), l'utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti *online* (Capo II); il principio e le regole di equa remunerazione di autori e artisti (interpreti o esecutori) nei contratti di sfruttamento (Capo III).

Con riguardo alla trasposizione nel diritto interno, il Decreto ha determinato importanti modifiche all'articolato della legge sul diritto d'autore (la l. 633/1941, "**l.a.**"), introducendo anche alcuni correttivi che in certi casi potrebbero apparire estranei alle intenzioni del legislatore europeo.

Con riferimento al contenuto del Titolo II della Direttiva, sono state introdotte nella l.a. nuove eccezioni e limitazioni ai fini di adeguamento ai nuovi mezzi e conseguente utilizzo di materiale protetto in ambiente digitale nei settori dell'istruzione, della ricerca e della conservazione del patrimonio culturale. In particolare, è stato introdotto l'articolo 70-*bis* l.a. che legittima taluni utilizzi di brani, parti di opere o altri materiali per attività svolte con mezzi digitali ed esclusivamente per finalità illustrative ad uso didattico. All'articolo 68 l.a. è aggiunto il comma 2-*bis* che legittima "sempre" l'eccezione al diritto di riproduzione e di realizzazione di copie di opere protette da parte degli istituti di tutela del patrimonio culturale per finalità di conservazione di tali opere. Simili eccezioni sono state pure introdotte con riferimento alle attività di *Text and Data mining* (TDM) agli articoli 70-*ter* e 70-*quater* l.a. Il TDM, in italiano 'estrazione di testo e di dati', è definito come "*qualsiasi tecnica automatizzata volta ad analizzare grandi quantità di testi, suoni, immagini, dati o metadati in formato digitale con lo scopo di generare informazioni, inclusi modelli, tendenze e correlazioni*" (art. 70-*ter*, co. 2 l.a.). Ai sensi dell'art. 70-*ter* co. 1 l.a., "*[s]ono consentite le riproduzioni compiute da organismi di ricerca e da istituti di tutela del patrimonio culturale, per scopi di ricerca scientifica, ai fini dell'estrazione di testo e di dati da opere o da altri materiali disponibili in reti o banche di dati cui essi hanno lecitamente accesso, nonché la comunicazione al pubblico degli esiti della ricerca ove espressi in nuove opere originali*". Per 'istituti di tutela del patrimonio culturale' si intendono "*le biblioteche, i musei, gli archivi, purché aperti al pubblico o accessibili al pubblico, inclusi quelli afferenti agli istituti di istruzione, agli organismi di ricerca e agli organismi di radiodiffusione pubblici, nonché gli istituti per la tutela del patrimonio cinematografico e sonoro e gli organismi di radiodiffusione pubblici*" (art. 70-*ter* co. 3 l.a.), mentre per 'organismi di ricerca' si intendono "*le università, comprese le relative biblioteche, gli istituti di ricerca o qualsiasi altra entità il cui obiettivo primario è quello di condurre attività di ricerca scientifica o di svolgere attività didattiche che includano la ricerca scientifica, che alternativamente:*

a) operino senza scopo di lucro o il cui statuto prevede il reinvestimento degli utili nelle attività di

ricerca scientifica, anche in forma di partenariato pubblico-privato;

b) perseguano una finalità di interesse pubblico riconosciuta da uno Stato membro dell'Unione europea", mentre non si considerano organismi di ricerca "*quelli sui quali è esercitata da imprese commerciali un'influenza determinante tale da consentire un accesso su base preferenziale ai risultati generati dalle attività di ricerca scientifica*" (art. 70-*ter* commi 4 e 5 l.a.).

Fuori dalla suddetta eccezione, dichiaratamente intesa a favorire gli scopi di ricerca scientifica perseguiti dai suddetti soggetti, la disciplina è disegnata dall'art. 70-*quater* l.a. in modo tale da dipendere sostanzialmente dalla volontà dei titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati. Ed infatti, ai sensi dell'art. 70-*quater* l.a., fuori dai casi dell'eccezione appena riferita, disciplinata dall'art. 70-*ter*, "*sono consentite le riproduzioni e le estrazioni da opere o da altri materiali contenuti in reti o in banche di dati cui si ha legittimamente accesso ai fini dell'estrazione di testo e di dati*", ma si soggiunge subito appresso che "*[l]'estrazione di testo e di dati è consentita quando l'utilizzo delle opere e degli altri materiali non è stato espressamente riservato dai titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati*". Numerose perplessità hanno accompagnato le previsioni della Direttiva in relazione all'effettiva portata del diritto di riproduzione e alla sua applicazione nel contesto di attività di TDM, così come in relazione alle nozioni di 'testo', 'dati' ed 'informazioni', non definiti nella Direttiva (e nemmeno nel Decreto), nonché in relazione recepimento nazionale, che, per certi aspetti, sembra essere anche più restrittivo della disciplina della Direttiva nel configurare l'ambito delle eccezioni e delle limitazioni. Si tratta comunque di una novità che ha una sicura importanza nel disegnare il rapporto tra diritti esclusivi e uso automatizzato delle opere.

Il Decreto, inoltre, interviene introducendo nella l.a. un nuovo Titolo II-*quinques*, a sostegno degli istituti di tutela del patrimonio culturale nella digitalizzazione e diffusione, anche transfrontaliera, delle opere e di altri materiali fuori commercio inserendo gli artt. da 102-*undecies* a 102-*septiesdecies* l.a., che dettagliano: la definizione di 'opere e di altri materiali fuori commercio' e le procedure per individuare ulteriori elementi per la definizione di opere fuori commercio; la gestione delle licenze collettive estese e l'applicazione dell'eccezione specifica; la risoluzione dei conflitti concernenti la disciplina delle opere orfane; la regolamentazione delle misure di pubblicità. Lo sfruttamento delle opere fuori commercio può avvenire solo ove l'istituto di tutela del patrimonio culturale (come definito dall'art. 70-*ter* l.a.), accertata la natura di opera o materiale fuori commercio, abbia richiesto all'organismo di gestione collettiva di cui al D.Lgs. 35/2017, rappresentativo dei titolari dei diritti per tipologia di opera o di diritto oggetto della licenza, il rilascio di una licenza a fini non commerciali per la riproduzione, la distribuzione, la comunicazione o la messa a disposizione al pubblico dell'opera.

Qualora il titolare dei diritti non abbia conferito mandato ad alcun organismo di gestione collettiva, la competenza al rilascio della licenza spetterà all'organismo che a livello nazionale sia sufficientemente rappresentativo dei titolari dei diritti, ovvero ai tre organismi maggiormente rappresentativi. Inoltre, i titolari dei diritti, ai sensi dell'art. 102-*quaterdecies* l.a., possono sempre ottenere l'esclusione delle loro opere dall'applicazione delle licenze collettive estese.

Uno degli articoli che in sede di recepimento ha fatto più discutere è l'articolo 14 della Direttiva, che liberalizza la riproduzione delle opere delle arti visive ormai cadute in pubblico dominio. La norma deriva dalla necessità di risolvere la specifica esigenza di dare effettività al pubblico dominio, liberalizzando le riproduzioni fotografiche che non abbiano carattere creativo, sorta in seguito ad una recente pronuncia della Corte di Giustizia Federale tedesca. La disposizione ha destato interrogativi con riguardo alle possibili modalità della sua trasposizione nel nostro ordinamento, alla luce del fatto che essa si pone in conflitto con la disciplina autorale della fotografia semplice (art. 87 l.a.) ed ancor di più con quanto disposto dal Codice dei beni culturali e del paesaggio (D.lgs. 22 gennaio 2004, n. 42, c.d. Codice Urbani), che sottopone ad una concessione la riproduzione di beni culturali per scopi commerciali (art. 108 Codice dei beni culturali e del paesaggio). Da parte dei sostenitori dell'*open access* alla cultura non erano mancate dichiarazioni di soddisfazione per l'intravista possibilità di una piena liberalizzazione della riproduzione del patrimonio culturale, che sarebbe seguita al recepimento della norma in questione, compresa la possibilità di realizzazione della c.d. libertà di panorama. Questa norma è oggi stata trasfusa nel nuovo articolo 32-*quater* l.a., che però, per un verso, si limita a recepire letteralmente il testo europeo, non consentendo di chiarire il rapporto con la disciplina nazionale della fotografia semplice, dall'altro fa espressamente salvo il regime del Codice dei beni culturali e del paesaggio: "*Alla scadenza della durata di protezione di un'opera delle arti visive, anche come individuate all'articolo 2, il materiale derivante da un atto di riproduzione*

di tale opera non è soggetto al diritto d'autore o a diritti connessi, salvo che costituisca un'opera originale. Restano ferme le disposizioni in materia di riproduzione dei beni culturali di cui al decreto legislativo 22 gennaio 2004, n. 42". La norma lascia integralmente in vigore le disposizioni confliggenti previste dal Codice Urbani, mancando così l'occasione di realizzare le intenzioni della Direttiva

Acceso è stato pure il dibattito antecedente al recepimento del successivo art. 15 della Direttiva, che introduce nell'*acquis* unionale un nuovo diritto connesso in favore degli editori *online*. L'intervento ha lo scopo di disciplinare il tema dell'utilizzo *online* dei contributi editoriali da parte dei prestatori di servizi della società dell'informazione come fenomeno potenzialmente lesivo del diritto d'autore. Il legislatore ha dunque previsto per gli editori un diritto connesso a quello dell'autore per la riproduzione e la messa a disposizione del pubblico di pubblicazioni di carattere giornalistico, sottoponendo la condivisione *online* degli stessi da parte dei prestatori dei servizi, ad una autorizzazione da parte dell'editore.

Non sono coperti da tale diritto connesso i collegamenti ipertestuali, le singole parole e gli estratti molto brevi; sono inoltre liberi gli utilizzi privati e non commerciali dell'opera in questione. L'articolo è stato recepito in sede nazionale agli artt. 43-*bis* e 70-*quinquies* l.a. È però presente, nel testo di recepimento una importante precisazione tutta italiana in relazione alla definizione di "*estratto molto breve di pubblicazione di carattere giornalistico*", per tale intendendosi una "*qualsiasi porzione di tale pubblicazione che non dispensi* [il lettore] *dalla necessità di consultazione dell'articolo giornalistico nella sua integrità*" (art. 43-*bis* co. 7 l.a.).

Le norme, in ossequio a quanto traspongono, riconoscono il diritto agli autori e agli editori ad una remunerazione. Tuttavia, la formulazione dell'obbligo, introdotto dal comma 8 dell'articolo 43-*bis* l.a., per i prestatori di servizi di corrispondere un "*equo compenso*" agli editori, ha fatto dubitare della sua conformità alla Direttiva e, sul piano nazionale, del rispetto dei limiti di cui alla legge delega che ha incaricato il Governo, per la circostanza che tale previsione sembra trasformare il diritto esclusivo degli editori a una sorta di diritto a un equo compenso. Il medesimo comma prevede anche che entro 60 giorni dall'entrata in vigore del Decreto l'AGCOM adotti un regolamento che individui i criteri per la determinazione del compenso. Proprio su questa ultima previsione, l'AGCM – in un più ampio parere sull'attuazione della Direttiva, espresso nell'adunanza del 31 agosto 2021 (https://www.agcm.it/dotcmsdoc/bollettini/2021/38-21.pdf) – si era espressa contrariamente, ritenendo l'intervento dell'autorità pubblica ingiustificatamente limitativo della libertà contrattuale degli operatori economici. L'AGCM aveva pertanto suggerito di demandare il compito di intermediazione agli organismi di gestione collettiva e alle entità di gestione indipendenti, ma il legislatore italiano non ha accolto il suggerimento.

Infine, l'articolo 17 della Direttiva, trasposto nel Titolo II- *quater* l.a., contiene il riconoscimento che, come sostenuto da tempo dalla giurisprudenza, i prestatori di servizi di condivisione di contenuti *online* effettuano un atto di comunicazione al pubblico o di messa a disposizione del pubblico in relazione agli atti di caricamento di materiali o di opere protette effettuato dai loro utenti (c.d. *user generated content*). Per questi atti non si applica il regime di esonero di responsabilità già previsto dalla Direttiva 2000/31/CE (c.d. direttiva sul commercio elettronico), con la conseguenza che, in assenza di una valida autorizzazione, i prestatori di servizi di condivisione di contenuti *online* devono porre in essere una serie di specifiche attività (*best efforts*) volte a garantire i diritti esclusivi degli autori, altrimenti incorrendo in responsabilità. A tale regime sono però affiancate delle eccezioni e delle fattispecie di esenzione parziale da responsabilità per certe tipologie di ISP. Di particolare interesse è il recepimento all'articolo 102-*decies* l.a. del procedimento di reclamo e ricorso, previsto dal comma 9 dell'art. 17 della Direttiva. Interessante segnalare che, come previsto dalla Direttiva, anche l'art. 102-*decies* l.a. prevede che le decisioni sulla richiesta di disabilitazione o la rimozione dei contenuti debbano essere soggette a "*verifica umana*". In più, però, il nostro legislatore ha scelto, in assenza di una simile disposizione della Direttiva, di disabilitare i contenuti fino al termine della procedura di reclamo, tutelando così maggiormente il titolare dei diritti (art. 102-*decies*, co. 3 l.a.: "*Nelle more della decisione sul reclamo, i contenuti in contestazione rimangono disabilitati*."). Inoltre si evidenzia che la gestione dei ricorsi è stata attribuita alla competenza di AGCOM che dovrà, entro 60 giorni dall'entrata in vigore del Decreto in argomento, emanare un regolamento *ad hoc*. È tuttavia precisato che è impregiudicato il diritto di ricorrere all'autorità giudiziaria (art. 102-*decies*, co. 4 l.a.).

In conclusione, è possibile ritenere che il Decreto introduca delle importanti novità alla disciplina del diritto d'autore, la cui concreta portata si coglierà nel prossimo futuro.

EMANUELA BURGIO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021-11-08;177

2. L'attuazione della direttiva "Open Data" (UE) 2019/1024, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (D.Lgs. 8 novembre 2021, n. 200, modificativo del D.Lgs. 36/2006)

Il 15 dicembre 2021 è entrato in vigore il D.Lgs. 8 novembre 2021, n. 200, recante le disposizioni di attuazione, nell'ordinamento italiano, della direttiva (UE) 2019/1024 del 20 giugno 2019, "*relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*" (c.d. direttiva *Open Data*), che ha abrogato la direttiva 2003/98/CE, "*relativa al riutilizzo dell'informazione del settore pubblico*".

La direttiva *Open Data* detta standard 'minimi' sul riutilizzo dei documenti – nella disponibilità di enti pubblici e di imprese pubbliche e private degli Stati Membri – contenenti dati pubblici, al fine di promuovere l'utilizzo dei 'dati aperti' e di incentivare la ricerca e l'innovazione. E l'art. 1 del D.Lgs. n. 200/2021, che a tale direttiva ha dato attuazione, ha recato importanti modifiche al D.Lgs. 24 gennaio 2006, n. 36, che aveva a propria volta recepito la direttiva 2003/98/CE. Ai sensi del D.Lgs. 36/2006, 'dato pubblico' è il "dato conoscibile da chiunque" e 'documento' è, secondo la definizione del medesimo Decreto Legislativo, come integrato dal D. Lgs. 200/2021, "la rappresentazione di atti, fatti e dati a prescindere dal supporto, cartaceo o elettronico, registrazione sonora, visiva o audiovisiva o qualsiasi parte di tale contenuto nella disponibilità della pubblica amministrazione o dell'organismo di diritto pubblico. La definizione di documento non comprende i programmi informatici".

Si riportano di seguito le principali novità introdotte dal nuovo articolo.

Il comma 2 prevede un'estensione dell'ambito applicativo del D.Lgs. n. 36/2006, tanto sul piano soggettivo che su quello oggettivo. In particolare, esso stabilisce, per un verso, che anche le imprese pubbliche e private sono tenute a rendere disponibili, ai fini del relativo riutilizzo, i documenti contenenti dati pubblici e, per altro verso, che il decreto trova altresì applicazione con riguardo ai 'dati della ricerca', agli altri dati nella disponibilità di imprese pubbliche e private che assolvano oneri od obblighi di servizio pubblico ovvero siano, in generale, gestori di servizi pubblici con riguardo ai servizi di pubblico interesse, nonché ai documenti ai quali si applica il D.Lgs. 27 gennaio 2010, n. 32.

Il comma 3 modifica alcune delle definizioni contenute nel decreto del 2006, da un lato, aggiornando riferimenti normativi ormai superati (come nel caso della definizione di 'pubblica amministrazione') e, d'altro lato, introducendo nuove definizioni, sulla scia di quanto previsto dalla direttiva: è il caso delle definizioni di 'anonimizzazione', 'dati dinamici', 'dati della ricerca', 'serie di dati di elevato valore' e 'riutilizzo', che si trovano nelle seguenti nuove lettere dell'art. 2 co. 1 D.Lgs. 36/2006 così formulate:

"c-*quinquies*) anonimizzazione: la procedura mirante a rendere anonimi documenti, rendendoli non riconducibili a una persona fisica identificata o identificabile, ovvero la procedura mirante a rendere anonimi dati personali in modo da impedire o da non consentire piu' l'identificazione dell'interessato;

c-*sexies*) dati dinamici: documenti informatici, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilita' o rapida obsolescenza;

c-*septies*) dati della ricerca: documenti informatici, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di come necessari per convalidare le conclusioni e i risultati della ricerca;

c-*octies*) serie di dati di elevato valore: documenti il cui riutilizzo è associato importanti benefici per la società, l'ambiente e l'economia, in considerazione della loro idoneità per la creazione di servizi, applicazioni a valore aggiunto e nuovi posti di lavoro, nonché del numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto basati su tali serie di dati; […]

e) riutilizzo: l'uso da parte di persone fisiche o giuridiche di documenti detenuti da:

1) pubbliche amministrazioni o organismi di diritto pubblico, per fini commerciali o per fini non commerciali, diversi da quelli istituzionali per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio di documenti tra pubbliche amministrazioni, o organismi di diritto pubblico, ovvero tra amministrazioni e organismi di diritto pubblico, posto in essere esclusivamente nell'ambito dell'espletamento dei compiti istituzionali di cui sono titolari;

2) imprese pubbliche e imprese private di cui all'articolo 1, comma 2-*quater*, per fini

commerciali o per fini non commerciali, diversi da quelli relativi alla fornitura dei servizi di interesse generale per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio di documenti tra imprese pubbliche e pubbliche amministrazioni o organismi di diritto pubblico posto in essere esclusivamente nell'ambito dell'espletamento dei compiti istituzionali delle pubbliche amministrazioni".

Il comma 4 introduce poi alcune modifiche alle esclusioni dall'ambito applicativo della disciplina. Tra queste, particolarmente rilevanti appaiono quelle relative ai documenti: *(i)* detenuti da imprese pubbliche, prodotti al di fuori della prestazione di servizi di interesse generale e/o connessi ad attività direttamente esposte alla concorrenza e non soggette alle norme in materia di appalti; *(ii)* esclusi dall'accesso procedimentale o dall'accesso civico semplice o generalizzato, ai sensi della normativa vigente; *(iii)* per i quali l'accesso è escluso, limitato o comunque pregiudizievole per la vita privata o l'integrità delle persone, alla luce delle norme in materia di protezione dei dati personali.

Il comma 6 riscrive integralmente il procedimento relativo all'esame della richiesta di riutilizzo dei documenti racchiuso all'art. 5 del decreto modificato. In particolare, stabilisce un termine di 30 giorni (prorogabile per ulteriori 20, "nel caso in cui le richieste siano numerose o complesse") ai fini dell'esame delle richieste: in caso di decisione positiva, i documenti sono resi disponibili al richiedente, ove possibile, in forma elettronica e, se necessario, mediante licenza. Avverso l'eventuale provvedimento di diniego, necessariamente motivato, il richiedente può esperire i mezzi di tutela previsti dall'art. 25, comma 4 e 5, della l. n. 241/1990.

Il nuovo art. 6 del D.Lgs. n. 36/2006, introdotto dal comma 7 dell'art. 1 D.Lgs. 36/2006, stabilisce poi che gli enti e le imprese pubbliche debbono mettere a disposizione i propri documenti in formato leggibile meccanicamente e aperto; con particolare riguardo ai dati dinamici e ai dati di elevato valore, i documenti devono essere messi a disposizione tramite adeguata *application programming interface* (API) e, ove possibile, mediante *download* in blocco.

Fermo il principio relativo alla gratuità della messa a disposizione dei dati, il comma 8 fa salva la possibilità per i detentori di richiedere un corrispettivo per il recupero dei costi marginali per le attività svolte a tal fine, nonché per l'anonimizzazione dei dati personali o per proteggere le informazioni commerciali di carattere riservato. Si fa poi rinvio a un decreto del Ministero dell'economia e delle finanze per l'individuazione dell'elenco dei soggetti esclusi dal principio di gratuità.

Il comma 9 novella l'art. 8 del D.Lgs. n. 36/2006, prevedendo l'adozione di licenze standard per il riutilizzo dei dati: si stabilisce, in particolare, che esse non devono subordinare il riutilizzo a condizioni, salvo queste siano obiettive, proporzionate, non discriminatorie e comunque giustificate da un pubblico interesse.

Il comma 11 introduce il nuovo art. 9-*bis* del D.Lgs. n. 36/2006, concernente il riutilizzo dei 'dati della ricerca' allorquando essi siano il risultato di attività di ricerca finanziata con fondi pubblici e quando gli stessi dati siano resi pubblici, anche attraverso l'archiviazione in una banca dati pubblica, da ricercatori, organizzazioni che svolgono attività di ricerca e organizzazioni che finanziano la ricerca, tramite una banca dati gestita a livello istituzionale o su base tematica. Esso prevede che tali dati debbano essere riutilizzabili a fini commerciali e no, in conformità a quanto previsto dal decreto e comunque nel rispetto della disciplina sulla protezione dei dati personali, degli 'interessi commerciali', dei diritti di proprietà intellettuale e di proprietà industriale. Inoltre, è prescritto che tali dati debbano rispettare i requisiti di reperibilità, accessibilità, interoperabilità e riutilizzabilità.

Quanto, poi, alla possibilità di stipulare accordi di esclusiva, il comma 13 – modificando l'art. 11 del D.Lgs. n. 36/2006 – prevede che essi possano essere conclusi solo ove necessari, ossia se per l'erogazione di un servizio d'interesse pubblico è necessario un diritto esclusivo, e che comunque la fondatezza del motivo di attribuzione dell'esclusiva sia soggetta a valutazione periodica (con cadenza almeno triennale). In ogni caso, tali accordi devono contenere termini trasparenti e pubblicati sul sito istituzionale prima che abbiano effetto. La disciplina dell'art. 11 trova applicazione anche con riferimento alle disposizioni che, pur non concedendo espressamente un'esclusiva, limitano la possibilità di riutilizzo dei documenti da parte di terzi rispetto all'accordo.

Il comma 14 modifica l'art. 12 del decreto del 2006, stabilendo che l'Agenzia per l'Italia digitale (AgID) adotti le linee guida contenenti le regole tecniche per l'attuazione del D.Lgs. n. 200/2021.

Il comma 15, infine, inserisce un nuovo articolo (12-*bis*) al D.Lgs. n. 36/2006, riguardante specifiche serie di dati di elevato valore, individuate dalla Commissione europea ai sensi dell'art. 14, paragrafo 1 della *Open Data Directive*. Tali serie debbono essere rese disponibili gratuitamente, leggibili meccanicamente, fornite mediante API e mediante *download* in blocco, se del caso.

Infine, gli articoli 2 e 3 del D.Lgs. n. 200/2021 prevedono, rispettivamente, l'abrogazione dell'art. 3 del D.Lgs. 18 maggio 2015, n. 102 (che aveva dato attuazione alla direttiva 2013/37/UE, modificativa della menzionata direttiva 2003/98/CE) e l'esclusione di nuovi o maggiori oneri per la finanza pubblica derivanti dall'attuazione del decreto.

RICCARDO ALFONSI

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021-11-08;200

3. L'attuazione della direttiva (UE) 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche (D. Lgs. 8 novembre 2021, n. 207, modificativo del D. Lgs. 259/2003)

Il 24 dicembre 2021 è entrato in vigore il Decreto Legislativo n. 207 dell'8 novembre 2021 (il "**Decreto**"), che dà attuazione alla direttiva (UE) 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche (innanzi anche solo il "**Codice**").

In precedenza, il 4 febbraio 2021, l'Italia insieme ad altri 24 Stati membri era stata sanzionata per il ritardo nel recepimento della direttiva, il cui termine finale era stato previsto per il 21 dicembre 2020.

Il Decreto va a sostituire i primi 98 articoli del Codice delle comunicazioni elettroniche (D. Lgs. 259/2003) e, di fatto, incide profondamente sulla previgente disciplina.

Esso, infatti, riguarda sia le reti e ed i servizi di comunicazione elettronica ad uso pubblico sia le reti ed i servizi di comunicazione elettronica ad uso privato, oltre a disciplinare il mercato delle reti di comunicazione per la diffusione circolare di programmi sonori e televisivi nonché tutti i servizi radioelettrici e a predisporre strumenti di tutela degli impianti sottomarini di comunicazione elettronica.

Le novità più rilevanti attengono agli obblighi di trasparenza imposti agli operatori, la durata dei contratti ed il diritto di recesso. Sono riconosciuti maggiori poteri all'Autorità per le Garanzie nelle Comunicazioni e si prevedono modifiche in materia edilizia.

In merito agli obblighi di trasparenza per gli operatori, a norma dell'art. 98-*septies decies* del Codice, «se il contratto prevede la proroga automatica di un contratto», essi informano «l'utente finale, in modo chiaro e tempestivo e su un supporto durevole, circa la fine dell'impegno contrattuale e in merito alle modalità di recesso dal contratto e migliori tariffe relative ai loro servizi», e sono tenuti almeno una volta all'anno ad aggiornare gli utenti finali in merito alle migliori tariffe.

Per quanto concerne la durata dei contratti, essa non può essere superiore ai 24 mesi, con l'obbligo in capo ai fornitori di prevedere che tra le offerte commerciali almeno una abbia una durata massima iniziale di 12 mesi.

Il diritto di recesso dell'utente viene rafforzato ulteriormente. Si prevede, difatti, che l'utente finale abbia il diritto di recedere dal contratto in qualsiasi momento con un preavviso di massimo un mese, nel caso in cui sia prevista la proroga automatica del contratto. In ogni modo, l'utente può esercitare il suo diritto di recesso entro sessanta giorni dall'avvenuta comunicazione di modifica delle condizioni contrattuali. Inoltre, i fornitori sono tenuti ad informare «gli utenti finali, con preavviso non inferiore a trenta giorni, di qualsiasi modifica delle condizioni contrattuali e, al contempo, del loro diritto di recedere dal contratto senza incorrere in alcuna penale né ulteriore costo di disattivazione se non accettano le nuove condizioni» (nuovo art. 98-*septies decies* del Codice).

Sono notevolmente ampliati i poteri sanzionatori concessi all'Autorità per le Garanzie nelle Comunicazioni, come si evince dall'art. 30 del Decreto. Nello specifico, l'AGCOM può emettere sanzioni amministrative pecuniarie nei confronti di imprese aventi significativo potere di mercato non inferiori al 2 per cento e non superiore al 5 per cento del fatturato realizzato nell'ultimo bilancio approvato anteriormente alla notificazione della contestazione e relativo al mercato al quale l'inottemperanza si riferisce.

Il Decreto affronta anche alcune questioni disciplinate dal testo Unico per l'edilizia. In particolare, per le nuove costruzioni e per gli interventi su edifici esistenti si richiede l'equipaggiamento digitale e l'attestazione tramite una specifica etichetta di «edificio predisposto alla banda ultra larga».

Inoltre, viene modificato anche l'art. 24 del testo Unico per l'edilizia dedicato all'agibilità degli edifici, sancendo che tra le condizioni della segnalazione certificata di agibilità rientra la certificazione dell'avvenuto rispetto degli obblighi di infrastrutturazione digitale.

In conclusione, si può notare che il nuovo Codice europeo delle comunicazioni elettroniche va ad incidere sia su profili concorrenziali del mercato sia sul fronte della tutela del consumatore, assumendo una prospettiva amplia di disciplina.

ENZO MARIA INCUTTI

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021;207

4. Verso il Data Act: la proposta di Regolamento del Parlamento e del Consiglio su regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati) COM(2022) 68 final del 23.2.2022

Con il documento COM(2022) 68 *final* del 23 febbraio 2022, recante "Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati)" (la "**Proposta di *Data Act***"), la Commissione europea ha pubblicato una proposta di regolamento che si aggiunge agli ormai numerosi interventi riferiti sin nella loro intitolazione ai "dati". Oltre al GDPR del 2016 "Regolamento generale sulla protezione dei dati" (Reg. UE 2016/679) possiamo citare il "Regolamento sulla libera circolazione dei dati non personali" del 2018 (Reg. UE 2018/1807), la direttiva "*Open Data"* del 2019 (Direttiva UE 2019/1024 relativa alla "apertura dei dati e al riutilizzo dell'informazione del settore pubblico" attuata da parte del legislatore italiano con D. Lgs. 8 novembre 2021 n. 200, su cui v. la notizia n. 2, *supra*, in questa Rubrica) e la Proposta di "*Data Governance Act"* del 2020, (Proposta di "regolamento relativo alla *governance* europea dei dati", del 25 novembre 2020) su cui v. la notizia n. 4 del numero 4/2021 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf.

La Proposta di *Data Act* comprende una bozza di regolamento (la "**Bozza di Regolamento**") ed una relazione esplicativa (la "**Relazione**").

Il **Capo I** della Bozza di Regolamento (artt. 1-2) ne definisce l'oggetto e il campo di applicazione e contiene le definizioni utilizzate nel corpo del provvedimento. In particolare, secondo l'art. 1 par. 1, il regolamento "stabilisce regole armonizzate sulla messa a disposizione all'utente di un prodotto o di un servizio correlato, di dati generati dall'uso di tale prodotto o servizio, sulla messa a disposizione di dati da parte dei *data holders* ai *data recipients*, e sulla messa a disposizione di dati da parte dei *data holders* a organi del settore pubblico o istituzioni dell'Unione, agenzie o organi, laddove si verifichi una necessità eccezionale, per l'esecuzione di un compito svolto nel pubblico interesse". L'art. 2 offre la stessa definizione di 'dati' contenuta nella Proposta di *Data Governance Act* del 2020, ossia "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva". Le definizioni di prodotto e di servizio correlato sono, rispettivamente, le seguenti: "'prodotto' significa un oggetto tangibile e mobile, anche se incorporato in un oggetto immobile, che ottiene, genera o raccoglie dati concernenti il suo uso o ambiente e che è capace di comunicare dati attraverso un servizio pubblicamente disponibile di comunicazione elettronica e la cui funzione primaria non consista nell' immagazzinamento e trattamento di dati", "'servizio correlato' significa un servizio digitale, compreso il *software*, che è incorporato o inter-connesso con un prodotto in modo tale che la sua assenza impedirebbe al prodotto di eseguire una delle sue funzioni". L' 'utente' è definito come "una persona fisica o giuridica che possiede, affitta o noleggia un prodotto o riceve un servizio". Il '*data holder'* è definito come "una persona giuridica o fisica che ha il diritto o l'obbligo, ai sensi di questo Regolamento, del diritto dell'Unione applicabile o del diritto nazionale che dà attuazione al diritto dell'Unione, o, in caso di dati non personali e attraverso il controllo del disegno tecnico del prodotto e dei servizi correlati, la capacità, di mettere a disposizione certi dati". Il '*data recipient*' è definito come "una persona giuridica o fisica, che agisce per fini connessi alla sua attività professionale, commerciale o artigianale, diversa dall'utente di un prodotto o di un servizio correlato, al quale il *data holder* mette a disposizione dati, inclusi terzi in conseguenza di una richiesta dell'utente al *data holder* o in conformità a un obbligo discendente dal diritto dell'Unione o dal diritto nazionale che dà attuazione al diritto dell'Unione". Tra le altre, l'art. 2 contiene anche una definizione di 'smart contract' quale "programma per elaboratore conservato in un sistema di registro elettronico laddove il risultato dell'esecuzione del programma è registrato nel registro elettronico" e rinvia per la definizione di 'registro elettronico' ad una definizione a sua volta oggetto della recente proposta della Commissione (COM(2021) 281 recante la "Proposta di un regolamento che modifichi il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea").

Il **Capo II** (artt. 3-7) è - secondo la Relazione - inteso ad aumentare la certezza per i consumatori e le imprese di accedere ai dati generati dai prodotti e dai servizi correlati che essi utilizzano. Secondo la sintesi contenutistica e finalistica indicata nella

Relazione, le norme di questo Capo prevedono che i prodotti e i servizi debbano essere progettati in un modo che renda i dati facilmente accessibili "*by default*" e che gli utenti debbano essere informati su quali dati sono accessibili e sulle modalità di accesso. L'art. 4 prevede che i dati debbano essere messi a disposizione dell'utente senza costi e, ove non direttamente accessibili, dietro semplice richiesta dell'utente. Sono previste alcune disposizioni che condizionano il diritto di accesso in relazione a segreti commerciali, come definiti dalla Direttiva (UE) 2016/943, e altre che vietano all'utente di utilizzare i dati ottenuti dal *data holder* per sviluppare prodotti che competono con il prodotto da cui generano i dati. Laddove si tratti di dati personali e l'utente non sia la persona interessata, il *data holder* può rendere tali dati personali accessibili all'utente soltanto nel rispetto delle condizioni previste dall'art. 6, par. 1 del GDPR, e, ove applicabile, dall'art. 9 del GDPR. Infine, l'art. 4 prevede che il *data holder* può utilizzare i dati non personali soltanto sulla base di un accordo con l'utente, e vieta al *data holder* di utilizzare i dati per trarne delle informazioni di natura economica, patrimoniale o industriale sull'utente che possano danneggiare la posizione commerciale dell'utente nei mercati in cui l'utente è attivo. L'art. 5 prevede il diritto dell'utente di chiedere al *data holder* di mettere i dati a disposizione di terzi senza spese per l'utente. L'art. 5 prevede che non possano agire per ottenere i dati ai sensi dell'art. 4 le imprese che forniscono servizi di piattaforma di base che hanno requisiti per qualificarsi come *gatekeepers* ai sensi del (non ancora approvato) *Digital Markets Act*, , sul quale v. la notizia 4 pubblicata sul numero 1/2021 di questa Rubrica (http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf). L'art. 6 prevede gli obblighi e i divieti in capo ai terzi ai quali vengono messi a disposizione i dati ai sensi dell'art. 5. È previsto che il trattamento dei dati da parte di questi soggetti debba essere limitato alle finalità e alle condizioni concordate con l'utente, nel rispetto dei diritti della persona interessata, relativamente ai dati personali, e con obbligo di cancellazione dei dati quando essi cessano di essere necessari per la finalità concordata. Tra i divieti è previsto anche in capo ai terzi il divieto di mettere i dati a disposizione di imprese che forniscono servizi di piattaforma di base che hanno i requisiti per qualificarsi come *gatekeepers* ai sensi del (non ancora approvato) *Digital Markets Act*. Infine, l'art. 7 dispone che gli obblighi di questo Capo non si applicano ai dati generati da prodotti realizzati o da servizi correlati prestati da piccole e microimprese (ai sensi dell'Articolo 2 dell'Allegato alla Raccomandazione 2003/361/CE).

Il **Capo III** (artt. 8-12) detta alcune regole da osservarsi allorquando i *data holders* sono obbligati (o sulla base di quanto previsto nel Capo II o sulla base di altre disposizioni del diritto dell'Unione o degli Stati membri) a mettere i dati a disposizione dei *data recipients*. Secondo la sintesi di cui alla Relazione, le disposizioni degli articoli 8 e 9 prevedono che le condizioni della messa a disposizione dei dati da parte dei *data holders* in favore dei *data recipients* debbano essere "*fair"* e non discriminatorie, e che, laddove sia previsto un corrispettivo, esso debba essere "*reasonable*", senza pregiudizio per altre disposizioni del diritto dell'Unione o del diritto nazionale derivato di escludere o ridurre un simile corrispettivo. È previsto in ogni caso che ai *data recipients* aventi le dimensioni di microimprese, piccole o medie imprese (come definite ai sensi dell'Articolo 2 dell'Allegato alla Raccomandazione 2003/361/CE) non possa essere chiesto un corrispettivo il cui importo ecceda i costi sopportati dai *data holders* per mettere i dati a loro disposizione, salvo che sia diversamente previsto nelle legislazioni di settore. L'art. 10 prevede che organi speciali, certificati dagli Stati membri, siano dedicati alla risoluzione di controversie tra *data holders* e *data recipients* aventi ad oggetto la determinazione delle condizioni di messa a disposizione dei dati ai sensi degli articoli 8 and 9.

Il **Capo IV** (composto del solo art. 13) intitolato "*Unfair terms related to data access and use between enterprises*" riguarda le clausole contrattuali concernenti l'accesso a dati o l'uso di dati o la responsabilità e i rimedi per l'inadempimento o l'estinzione di obbligazioni relative a dati, che siano "imposte unilateralmente" da imprese a microimprese, piccole o medie imprese (come definite ai sensi dell'Articolo 2 dell'Allegato alla Raccomandazione 2003/361/CE). L'art. 13 ricalca la terminologia e la tecnica normativa della direttiva 93/13/CEE sulle clausole abusive nei contratti stipulati con i consumatori. Secondo la sintesi della Relazione, l'obiettivo è quello di impedire che gli accordi contrattuali sull'accesso ai dati e l'uso di dati consentano di profittare di squilibri nel potere negoziale tra le parti contraenti. Lo strumento del test di "*unfairness*" prevede una definizione generale di abusività e due elenchi di clausole, uno relativo a clausole da intendersi in ogni caso abusive (tra cui quelle che consentono al predisponente di determinare la "conformità dei dati al contratto") e l'altro di clausole che si presumono abusive. L'art. 34 (contenuto nel Capo IX) prevede che la

Commissione debba predisporre e raccomandare modelli non vincolanti di contratto sull'accesso ai dati e l'uso di dati come strumento di ausilio alle parti nella redazione e negoziazione di contratti con diritti e doveri contrattuali equilibrati.

Il **Capo V** (artt. 14-22) è inteso a creare, secondo la presentazione della Relazione, un quadro armonizzato di regole per l'uso da parte di organi del settore pubblico e istituzioni dell'Unione di dati detenuti da imprese in situazioni nelle quali si riscontra una esigenza eccezionale dei dati richiesti. Il quadro si basa su un obbligo di mettere i dati a disposizione che sorge solo in caso di emergenze pubbliche ovvero in situazioni in cui gli organi del settore pubblico hanno una esigenza eccezionale di utilizzare certi dati, ma tali dati non possono ottenersi sul mercato, o in modo tempestivo attraverso l'emanazione di una nuova legislazione o per mezzo di obblighi già esistenti. È previsto che nel caso di un'esigenza eccezionale di rispondere ad una emergenza pubblica, come emergenze di salute pubblica o grandi disastri naturali o indotti dall'uomo, i dati dovranno essere messi a disposizione gratuitamente. In altri casi di esigenza eccezionale, incluso il caso di esigenze legate alle conseguenze di una emergenza pubblica, il *data holder* che mette i dati a disposizione ha diritto a una remunerazione comprensiva dei costi più un margine ragionevole. Per evitare abusi, è previsto che le richieste debbano essere proporzionate, che esse debbano indicare chiaramente gli obiettivi che si intendono perseguire e che rispettino gli interessi dei *data holder* che mettono i dati a disposizione. È previsto che autorità competenti *ad hoc* siano investiti del compito di assicurare la trasparenza e la pubblicazione di tutte le richieste e di gestire le relative eventuali doglianze.

Il Capo **VI** (artt. 23-26) prevede in capo ai fornitori di servizi *cloud*, *edge* ed altri servizi di trattamento di dati una serie di requisiti di natura contrattuale, commerciale e tecnica al fine di consentire la commutazione tra tali servizi. In particolare, la Proposta di *Data Act*, secondo la Relazione, mira ad assicurare che i clienti mantengano un minimo livello di funzionalità del servizio dopo che essi hanno ottenuto la commutazione in favore di un altro fornitore del servizio. La Proposta di *Data Act* contiene una eccezione per il caso di impraticabilità tecnica della commutazione, ma pone l'onere della prova al riguardo in capo al fornitore del servizio. La Proposta di *Data Act* non prevede standard tecnici delle interfacce, ma richiede che i servizi siano compatibili con gli standards europei, o, ove disponibili, con le specificazioni tecniche di interoperabilità aperta.

Il **Capo VII** (composto del solo art. 27) mira a contrastare l'accesso illegittimo ai dati non personali detenuti nell'Unione da fornitori di servizi di trattamento dei dati offerti nel mercato dell'Unione. Al riguardo sono previsti in capo ai fornitori di servizi di trattamento dei dati una serie di obblighi di salvaguardia di natura tecnica, legale e organizzativa.

Il **Capo VIII** (artt. 28-30) prevede alcune prescrizioni relative all'interoperabilità per gli operatori di "*data spaces*" e per i fornitori di servizi di trattamento di dati nonché alcuni requisiti per gli *smart contracts*.

Il **Capo IX** (art. 31 -34) prevede *inter alia* che gli Stati membri designino una o più autorità competenti per l'applicazione delle disposizioni del Regolamento, per l'esame di doglianze nonché per l'irrogazione di sanzioni per il caso di violazioni delle medesime disposizioni.

Il **Capo X** (composto del solo art. 35) prevede che il diritto *sui generis* di cui alla direttiva sulle banche di dati (Direttiva 96/9/CE) non si applichi alle banche di dati ottenute o generate dall'uso di un prodotto o di un servizio correlato. La Relazione spiega che tale previsione mira ad evitare che possano essere compromessi i diritti degli utenti ai sensi degli articoli 4 e 5 del Regolamento.

Infine, il **Capo XI** permette alla Commissione di adottare atti delegati per introdurre un meccanismo di monitoraggio sulle tariffe di commutazione imposte ai fornitori di servizi di trattamento di dati, al fine di specificare i requisiti essenziali riguardanti l'interoperabilità, e di pubblicare informazioni relative alle specificazioni e agli standard di interoperabilità. Si prevede inoltre l'adozione di specifiche tecniche comuni per gli *smart contracts* per l'ipotesi di carenza o insufficienza di *standards* armonizzati idonei a garantire la conformità ai requisiti essenziali previsti dal Regolamento.

SALVATORE ORLANDO

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN

5. La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022.

Il 26 gennaio 2022 la Commissione ha proposto una dichiarazione solenne interistituzionale sui diritti e i principi digitali per il decennio digitale: la

Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, del Parlamento europeo, del Consiglio e della Commissione (di seguito anche la "**Dichiarazione**"). Alla base della proposta, c'è la consapevolezza che l'accelerazione della trasformazione digitale e il suo pervadere ogni aspetto della vita delle persone rende sempre più importante che l'Unione Europea specifichi come applicare i suoi valori e i diritti fondamentali nel mondo *online*, non solo con provvedimenti puntuali e relativi a singoli settori, ma anche in modo trasversale e generale.

Il modello di trasformazione digitale auspicato mira a "rafforzare la dimensione umana dell'ecosistema digitale", nel pieno rispetto dei diritti fondamentali, del diritto alla protezione dei dati e alla non discriminazione, nonché dei principi di inclusività e di neutralità tecnologica e della rete. Il modello proposto è imperniato sul mercato unico digitale e basato su una tecnologia che contribuisca alla lotta ai cambiamenti climatici e alla protezione dell'ambiente. Sul punto la proposta *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* si pone in continuità con la *Dichiarazione di Tallinn sull'e-government*, firmata il 6 Ottobre 2017 da tutti gli Stati membri dell'UE e dai paesi dell' *European Free Trade Association (EFTA)* (https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration), con la *Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori*, firmata l'8 Dicembre 2020 dai ministri responsabili di tutti gli Stati membri dell'UE (https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government) e con la *Dichiarazione di Lisbona - "Democrazia digitale con uno scopo"*, presentata all'Assemblea sul digitale nel Giugno 2021 (https://futurium.ec.europa.eu/en/digital-compass/digital-principles/library-video/lisbon-declaration-digital-democracy-purpose?language=it-video/lisbon-declaration-digital-democracy-purpose?language=it).

La Dichiarazione si articola in sei capitoli, che hanno i seguenti contenuti.

Capitolo I: mettere le persone al centro della trasformazione digitale. Al fine di mettere concretamente le persone al centro della trasformazione digitale occorre impegnarsi a:

– rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita di tutti gli europei;

– adottare le misure necessarie per garantire che i valori dell'Unione e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati *online* così come *offline*;

– promuovere un'azione responsabile e diligente da parte di tutti gli attori digitali, pubblici e privati, per un ambiente digitale sicuro e protetto;

– promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali.

Capitolo II: solidarietà e inclusione. Il dovere di rispettare la persona umana e la sua dignità prescindono dal luogo o dal tempo nel quale ciascuno esplica la sua personalità.

La dimensione *online* delle nostre vite non può certamente prescindere dalla solidarietà e dall'inclusione. Anche le soluzioni tecnologiche devono, pertanto, consentire l'esercizio dei diritti, promuovere l'inclusione e "perseguire una trasformazione digitale che non lasci indietro nessuno, che includa in particolare gli anziani, le persone con disabilità, le persone emarginate, vulnerabili o prive di diritti, così come coloro che agiscono per loro conto".

A tal fine è necessario che tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutti gli europei.

La solidarietà e l'inclusione nel mondo digitale non possono prescindere dalla **connettività** digitale ad alta velocità a prezzi accessibili, indipendentemente dal luogo in cui le persone vivono e dal loro reddito, garantendo un'internet neutra e aperta in cui le applicazioni, i servizi e i contenuti non siano bloccati o degradati in modo ingiustificato. L'**inclusione** non può che realizzarsi attraverso il diritto all'istruzione, alla formazione e all'apprendimento al fine di acquisire **competenze digitali** di base e comunque necessarie per partecipare attivamente all'economia, alla società e ai processi democratici.

Le competenze digitali sono uno dei quattro punti cardine della proposta di decisione presentata dalla Commissione *"Path to the Digital Decade"* del 15 Settembre 2021 (https://ec.europa.eu/commission/presscorner/detail/it/ip_21_4630). Neppure si può prescindere da **condizioni di lavoro** eque, giuste, sane e sicure e, a tal fine, occorre proteggere il lavoratore nell'ambiente digitale, così come nel luogo di lavoro fisico, garantendo che tutti abbiano la possibilità di disconnettersi e di godere di garanzie per l'equilibrio tra vita professionale e vita privata. Ogni persona dovrebbe avere **accesso a tutti i servizi pubblici principali *online*** in tutta l'Unione.

A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo. Strategica diventa a tal fine la garanzia di un'identità digitale accessibile, sicura, affidabile e che consenta l'accesso ai servizi *online*, alle informazioni della Pubblica amministrazione ed ai servizi sanitari e assistenziali digitali concepiti per soddisfare le esigenze dei cittadini, comprese le cartelle cliniche.

Capitolo III: libertà di scelta. Nella Dichiarazione emerge la consapevolezza che gli algoritmi influenzano così tanto la nostra vita, dagli aspetti più insignificanti a quelli più importanti, che è persino la libertà di scelta a risentirne, a volte anche inconsapevolmente. Il Capitolo III della Dichiarazione infatti, dedicato alla libertà di scelta, si apre con il riferimento a **Interazioni con algoritmi e sistemi di intelligenza artificiale.**

Ogni persona, si legge, "dovrebbe essere messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali".

A tal fine occorre garantire:

– la trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone, quando interagiscono con essi, siano autonome, responsabili e informate;

– che i sistemi algoritmici siano basati su insiemi di dati adeguati, al fine di evitare discriminazioni illecite, e consentano la supervisione umana dei risultati che riguardano le persone;

– che le tecnologie come gli algoritmi e l'intelligenza artificiale non siano utilizzate per predeterminare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata;

– che i sistemi digitali e di intelligenza artificiale siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali delle persone.

A tal fine devono essere ben definite le responsabilità delle piattaforme, in particolare dei grandi operatori e dei *gatekeeper*, e deve garantirsi che ogni persona possa scegliere realmente quali servizi *online* utilizzare, sulla base di informazioni obiettive, trasparenti e affidabili.

Capitolo IV: partecipazione allo spazio pubblico digitale. Quanto detto per l'inclusione e la solidarietà vale anche per la libertà di espressione che non può certo essere mortificata per il fatto che si esplichi *online*. Ogni persona dovrebbe avere accesso a un ambiente *online* affidabile, sicuro, diversificato e multilingue. L'accesso a contenuti diversificati contribuisce a un dibattito pubblico pluralistico e dovrebbe consentire a tutti di partecipare al processo democratico. Ogni persona dovrebbe disporre dei mezzi per sapere chi possiede o controlla i servizi mediatici che utilizza. Il ruolo delle piattaforme online, specialmente se di grandi dimensioni, è ormai innegabile, godendo le stesse di un'autorità di fatto e di uno statuto privatistico che mal si concilia con la loro attività potenzialmente capace di produrre effetti rilevanti anche sul piano pubblicistico e istituzionali. Le piattaforme online di dimensioni molto grandi dovrebbero sostenere il libero dibattito democratico online, visto il ruolo svolto dai loro servizi nel plasmare l'opinione pubblica e il dibattito pubblico. Dovrebbero attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi, anche in relazione alle campagne di disinformazione, e tutelare la libertà di espressione.

A tal fine occorre adottare misure volte a contrastare tutte le forme di contenuti illegali proporzionatamente al danno che possono causare e nel pieno rispetto del diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza. Si evocano sul punto le scelte fatte con la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 *final* del 15 dicembre 2020, nota come *Digital Services Act*. (su cui v. la notizia n. 3 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf).

Capitolo V: sicurezza, protezione e conferimento di maggiore autonomia e responsabilità. Un ambiente online sicuro e protetto è un ambiente nel quale tecnologie, prodotti e servizi digitali, già nella fase di progettazione, sono tali da tutelare la **vita privata delle persone,** la loro **identità digitale** e il diritto alla protezione dei propri dati personali *online*. Tale diritto comprende il **controllo individuale sui dati**, su come sono utilizzati e sui soggetti con i quali sono condivisi. Ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e nessuno può essere sottoposto a misure illecite di sorveglianza o intercettazione *online*.

Ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, alle informazioni pubblicamente disponibili che la riguardano.

Particolarmente delicato è il problema della garanzia di una partecipazione *online* adeguata all'età; problema che la Dichiarazione non trascura,

allorché prevede che **i bambini e i giovani *online* dovrebbero essere protetti e dotati di maggiore autonomia e responsabilità**. Anche a tal fine non si può prescindere da offrire adeguate opportunità per consentire ai giovani, anche minori, capacità e competenze necessarie per navigare nell'ambiente *online* in modo attivo e sicuro, per compiere scelte informate *online* e esprimere, anche in tale ambito, la propria creatività.

Soprattutto con riferimento a questi soggetti, potenzialmente più vulnerabili degli adulti, non si può prescindere da strumenti idonei a proteggerli dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi *online*, impedendo che lo spazio digitale sia utilizzato per commettere o facilitare reati.

I minori hanno il diritto di essere protetti da tutti i reati commessi o facilitati attraverso le tecnologie digitali.

Capitolo VI: sostenibilità. Favorire lo sviluppo e l'utilizzo di tecnologie digitali sostenibili significa favorire lo sviluppo e l'utilizzo di tecnologie che abbiano un impatto ambientale minimo e sviluppare e diffondere soluzioni digitali con ricadute positive per l'ambiente e il clima.

A tal fine è necessario promuovere un'economia circolare nella quale prodotti e servizi digitali siano progettati, prodotti, utilizzati, smaltiti e riciclati in modo da ridurre al minimo il loro impatto negativo a livello ambientale e sociale.

Soprattutto è necessario consentire ad ogni persona di dare un contributo concreto alla sostenibilità e attraverso le proprie scelte. Ma ciò è possibile solo se è consentito a ciascuno di avere accesso a informazioni precise e di facile comprensione sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, in modo da essere in grado di compiere scelte responsabili.

SARA TOMMASI

https://digital-strategy.ec.europa.eu/en/news/commission-puts-forward-declaration-digital-rights-and-principles-everyone-eu

6. La proposta di Regolamento del Parlamento e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica COM(2021) 731 final del 25 novembre 2021

Con il documento COM(2021) 731 *final* del 25 novembre 2021, recante "Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica", la Commissione europea ha pubblicato una proposta di regolamento in materia di "pubblicità politica" che comprende una bozza di regolamento (la "**Bozza di Regolamento**") ed una relazione esplicativa (la "**Relazione**").

Nella Relazione, è specificato che scopo della proposta è contribuire al buon funzionamento del mercato interno della pubblicità politica con norme armonizzate – indirizzate ai prestatori di servizi di pubblicità politica - che garantiscano un livello di trasparenza elevato della pubblicità politica e servizi connessi. Altro scopo della proposta, indicato nella Relazione, è quello di tutelare le persone fisiche con riguardo al trattamento dei dati personali, in particolare attraverso norme sull'uso delle tecniche di *targeting* e della c.d. "amplificazione" sempre in ambito di pubblicità politica. La Bozza di Regolamento prevede che tali norme si applicheranno a tutti i titolari del trattamento - quindi non solo ai prestatori di servizi di pubblicità politica - che fanno uso delle tecniche di *targeting* e "amplificazione". L'art. 2 della Bozza di Regolamento definisce le 'tecniche di targeting o amplificazione' come segue: "*le tecniche usate per rivolgere solo a una persona specifica o a un gruppo specifico di persone un messaggio di pubblicità politica concepito su misura, o per aumentarne la diffusione, la portata o la visibilità*".

Nella Relazione si osserva che i servizi di pubblicità politica sono in fase di espansione nell'UE, e che, a fronte di ciò, il quadro, già molto frammentato, delle norme nazionali, è reso ancor maggiormente frammentario dalle innovazioni tecnologiche della comunicazione e dalla necessità degli Stati membri, di dare risposte alle nuove, conseguenti, forme della pubblicità politica. La Relazione riconosce che i dati personali dei cittadini dell'Unione sono utilizzati per indirizzare messaggi politici e per amplificarne l'impatto e la diffusione, con precisi rischi di ripercussioni negative sui diritti fondamentali dei cittadini, tra cui la libertà di opinione e informazione, nel prendere decisioni politiche ed esercitare il diritto di voto.

Nella Relazione si affronta il tema della coerenza della proposta con le disposizioni vigenti nel settore interessato e con le altre normative dell'Unione, così come si dà conto della base giuridica utilizzata, della sussidiarietà (per competenza non esclusiva), della proporzionalità e si motiva quindi in merito allo strumento del regolamento. Nell'ambito dell'esposizione sulla valutazione di impatto, la Relazione dichiara che le misure proposte hanno tutte un impatto positivo sui diritti fondamentali, ovvero che eventuali impatti

negativi non dovrebbero essere significativi. In particolare, a questo riguardo, la Relazione osserva e dichiara che la proposta impone restrizioni limitate alla libertà di espressione e di informazione (art. 11 della Carta dei diritti fondamentali dell'Unione europea "**CDFUE**"), al diritto alla vita privata (art. 7 CDFUE) e al diritto alla protezione dei dati di carattere personale (art. 8 CDFUE), ma soggiunge che tali restrizioni sono proporzionate e limitate al minimo necessario.

Il **Capo I** della Bozza di Regolamento (artt. 1-3) ne definisce l'oggetto e il campo di applicazione, contiene le definizioni dei termini principali e il livello di armonizzazione delle misure.

Il **Capo II** (artt. 4-11) tratta degli obblighi di trasparenza applicabili alla pubblicità politica a pagamento; stabilisce le misure applicabili a tutti i prestatori di servizi di pubblicità politica che concorrono alla preparazione, collocazione, promozione, pubblicazione o diffusione di pubblicità politica; in particolare dispone in ordine alla trasparenza della pubblicità politica (art. 4), all'obbligo di identificare i messaggi di pubblicità politica (art. 5) e all'obbligo di registrare e trasmettere informazioni agli editori di pubblicità politica (art. 6). In questo capo si prevedono anche ulteriori obblighi applicabili ai soli editori di pubblicità politica, in aggiunta a quelli di cui agli articoli 4, 5 e 6. In particolare, gli editori devono includere in ciascun messaggio di pubblicità politica una dichiarazione attestante chiaramente che si tratta di pubblicità politica, indicare il nome dello sponsor e pubblicare informazioni che rendano comprensibili il contesto più ampio in cui si situa il messaggio e i suoi obiettivi (art. 7). Gli editori di pubblicità politica devono inoltre pubblicare annualmente informazioni sugli importi fatturati e sul valore di altre prestazioni percepite in cambio parziale o integrale dei servizi prestati in relazione a messaggi di pubblicità politica (art. 8), e devono infine mettere in atto meccanismi di facile uso perché i cittadini possano segnalare i messaggi di pubblicità politica che non rispettano gli obblighi stabiliti dal regolamento (art. 9).

Gli artt. 10 e 11 prevedono che i prestatori di servizi di pubblicità politica devono trasmettere le informazioni pertinenti alle autorità competenti e ad altri soggetti interessati come previsti nell'art. 11.

Il **Capo III** (artt. 12-13), intitolato "*Targeting e amplificazione della pubblicità politica"* disciplina l'uso delle 'tecniche di *targeting* o amplificazione' che comportano il trattamento di dati personali a fini di pubblicità politica. È previsto che quando il trattamento riguarda dati sensibili, scatta un divieto cui è possibile derogare solo a precise condizioni. È inoltre prescritto ai responsabili del trattamento che ricorrono a queste tecniche a fini di pubblicità politica di adottare e applicare un "documento di strategia interna che in particolare descriva chiaramente e con linguaggio semplice l'uso di tecniche finalizzate a prendere di mira certi destinatari o amplificare l'impatto", tenere registri e trasmettere informazioni che permettano agli interessati di comprendere la logica utilizzata e i principali parametri della tecnica applicata e se siano stati usati dati di terzi e altre tecniche analitiche (art. 12). L'articolo 12 stabilisce inoltre ulteriori obblighi a carico degli editori di pubblicità politica. Infine, l'art. 13 prevede che i responsabili del trattamento debbano trasmettere le informazioni ai soggetti interessati ex art. 11.

Il **Capo IV** (artt. 14-17) prevede disposizioni concernenti il controllo e l'esecuzione del regolamento. Si impone ai prestatori di servizi di pubblicità politica non stabiliti nell'Unione l'obbligo di nominare un rappresentante legale in uno degli Stati membri in cui prestano i loro servizi (art. 14). Si stabilisce quali autorità debbano essere incaricate del controllo ed esecuzione delle misure specifiche stabilite dal regolamento. Si fa obbligo agli Stati membri di garantire la cooperazione tra le pertinenti autorità competenti. Si chiede che siano designati punti di contatto ai fini del regolamento e incarica gli Stati membri di garantire lo scambio di informazioni tra gli stessi (art. 15). Si prevede che gli Stati membri debbano stabilire norme sulle sanzioni applicabili in caso di inosservanza degli obblighi dettati dal regolamento (art. 16). Si stabilisce infine l'obbligo in capo agli Stati membri di "pubblicare in luogo visibile le date dei rispettivi periodi elettorali nazionali" (art. 17).

Il **Capo V** (artt. 18-20) contiene le disposizioni finali.

SALVATORE ORLANDO

https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0013.02/DOC_1&format=PDF

7. Il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 sull'iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale.

Il 17 febbraio 2022 è stato pubblicato sulla Gazzetta Ufficiale il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 (il "**Decreto**"). Esso disciplina l'iscrizione alla

sezione speciale del registro dei cambiavalute (il "**Registro**") tenuto dall'Organismo Agenti e Mediatori (l'"**OAM**") dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale (i "**Prestatori di servizi**").

Il Decreto attua l'art. 17-*bis*, comma 8-*ter* D. Lgs. 141/2010 che, insieme al comma 8-*bis* del medesimo articolo, sostanzialmente estende la disciplina dei cambiavalute ai Prestatori di servizi ed è stato introdotto dal D. Lgs. 90/2017 attuativo della direttiva 2015/849/UE (c.d. IV direttiva antiriciclaggio) e modificativo del D. Lgs. 231/2007 e del D. Lgs. 109/2007, e a sua volta modificato dal D. Lgs. 125/2019 attuativo della direttiva 2018/843/UE (c.d. V direttiva antiriciclaggio).

Per quanto qui interessa, l'art. 17-*bis*, commi 8-*bis* e *ter* D. Lgs. 141/2010 impone ai Prestatori di servizi di comunicare la loro operatività in Italia, nonché di iscriversi al Registro. Il suddetto comma 8-*ter*, in particolare, delegava ad un decreto del Ministero dell'economia e delle finanze, quello in commento appunto, di stabilire: 1) i tempi e i modi con cui i Prestatori di servizi devono comunicare la propria operatività sul territorio nazionale al suddetto Ministero; 2) le forme di cooperazione tra tale ultimo ente e le forze di polizia per impedire l'esercizio abusivo delle attività relative all'utilizzo di valuta virtuale e di portafoglio digitale.

L'art. 1 del Decreto, similmente al D. Lgs. 231/07, definisce:

(i) il prestatore di servizi relativi all'utilizzo di valuta virtuale come il soggetto "*che fornisce a terzi, a titolo professionale, anche on-line, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore … nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute*";

(ii) il prestatore di servizi di portafoglio digitale come colui "*che fornisce, a terzi, a titolo professionale, anche on-line, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti al fine di detenere … e trasferire valute virtuali*";

(iii) la valuta virtuale come "*la rappresentazione digitale di valore, non emessa né garantita da una banca centrale … non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente"*.

Ebbene, da quanto detto emerge che solo i soggetti i quali svolgano "professionalmente" una delle menzionate attività devono ottemperare al provvedimento in parola.

L'art. 3, comma 1 del Decreto stabilisce che i Prestatori di servizi per poter svolgere la propria attività in Italia debbano iscriversi nel Registro. Per farlo, innanzitutto, devono possedere i requisiti di cui all'art. 17-*bis*, comma 2 D. Lgs. 141/2010, ossia la cittadinanza di uno Stato dell'Unione europea, se si tratta di persone fisiche, oppure la sede legale e amministrativa o stabile organizzazione in Italia, se si tratta di persone giuridiche. In secondo luogo, devono inviare una comunicazione all'OAM sulla loro operatività in Italia, verosimilmente prima dell'inizio dell'attività anche se il Decreto non lo specifica. Tale adempimento, ai sensi del combinato disposto degli artt. 17 bis, comma 8 ter D. Lgs. 141/2010 e 3, comma 2 del Decreto, è una condizione essenziale affinché i Prestatori di servizi possano esercitare legittimamente la loro attività.

Coloro i quali siano già operativi alla data di avvio della sezione speciale del registro dei cambiavalute possono inviare la predetta comunicazione entro 60 giorni da tale data. Altrimenti, la loro attività si considera svolta abusivamente (art. 3, comma 3).

La comunicazione, sostanzialmente, deve indicare: i dati del Prestatore di servizi, la tipologia di attività o di servizio forniti e le modalità di svolgimento (art. 3, comma 4). L'OAM verifica la regolarità e completezza della comunicazione ed entro 15 giorni dal ricevimento "*dispone ovvero nega l'iscrizione*" nella sezione speciale del registro dei cambiavalute (art. 3, comma 6). Tale termine può essere sospeso una sola volta per massimo 10 giorni "*qualora l'OAM ritenga la comunicazione incompleta ovvero ritenga necessario integrare la documentazione*" ad essa allegata. Il diniego all'iscrizione, comunque, non impedisce di inviare una nuova comunicazione (art. 3, comma 7).

La sezione speciale del registro dei cambiavalute sarà istituita entro 90 giorni dall'entrata in vigore del Decreto da parte dell'OAM che ne cura "*la chiarezza, la completezza e l'accessibilità al pubblico dei dati*" e dispone di poteri di sospensione e cancellazione dal Registro medesimo (art. 4, commi 1, 2 e 5). Quest'ultimo riporta i dati relativi al Prestatore di servizi e alla tipologia di attività svolta (meglio descritta nell'Allegato 2 al Decreto), i punti fisici di operatività e/o l'indirizzo web tramite cui è offerto il servizio relativo all'utilizzo di valuta virtuale e di portafoglio digitale (art. 4, comma 3).

Trimestralmente, i Prestatori di servizi iscritti al Registro devono comunicare all'OAM i dati dei

loro clienti e delle operazioni effettuate per loro conto, come specificati nell'Allegato 1 al Decreto (art. 5).

Semestralmente, inoltre, anche sulla base delle informazioni trasmesse ex art. 5 del Decreto, l'OAM deve inviare al Ministero dell'economia e delle finanze una relazione contenente: 1) il numero di soggetti che hanno trasmesso la comunicazione per l'iscrizione al Registro, anche se non l'abbiano poi ottenuta; 2) la tipologia di servizi prestati dagli iscritti; 3) le ipotesi di esercizio abusivo dell'attività; 4) i dati aggregati trasmessi dai Prestatori di servizi all'OAM sulle operazioni da essi effettuate (art. 3, comma 8).

Ai sensi del combinato disposto degli artt. 4, comma 4 e 6, comma 1 del Decreto, l'OAM collabora coi soggetti di cui all'art. 21, comma 2 D. Lgs. 231/07 fornendogli "*tempestivamente*", su richiesta, ogni informazione e documento riguardante i Prestatori di servizi "*detenuta in forza della gestione della sezione speciale del registro"*, ivi compresi i dati trasmessi all'OAM ex art 5 del Decreto. I soggetti di cui all'art. 21, comma 2 D. Lgs. 231/07 includono: Ministero dell'economia e delle finanze, Autorità di vigilanza di settore, Unità di Informazione Finanziaria per l'Italia, Direzione investigativa antimafia, Guardia di finanza che operi tramite il Nucleo Speciale di Polizia Valutaria.

Le forze di polizia che rilevino l'esercizio abusivo di servizi relativi all'utilizzo di valuta virtuale o di portafoglio digitale possono accertare e contestare la violazione ai sensi della L. n. 689/81 (art. 6, comma 2).

Per quanto qui interessa, infine, occorre dare atto che il 18 febbraio 2022 l'OAM ha diffuso un comunicato stampa con cui sostanzialmente riassume i contenuti del Decreto e, soprattutto, informa che la sezione speciale del registro dei cambiavalute sarà attivata entro il 18 maggio 2022.

EMANUELE STABILE

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2022-02-17&atto.codiceRedazionale=22A01127&elenco30giorni=true

8. La decisione del 10 febbraio 2022 del garante privacy italiano sul trattamento di dati biometrici da parte di Clearview AI

Dopo la CNIL, l'autorità di controllo francese, che il 16 dicembre 2021 ha dichiarato illecito il trattamento di dati personali effettuato dalla società Clearview AI e imposto la cessazione della raccolta e trattamento di dati personali sul territorio francese, anche l'autorità italiana, il Garante per la protezione dei dati personali (di seguito il "**Garante**"), è intervenuto con provvedimento in data 10 febbraio 2022 accertando l'illiceità della raccolta di dati biometrici operata dalla medesima società e comminando una sanzione pecuniaria di 20 milioni di euro. In precedenza, Clearview AI era stata assoggettata ad un analogo provvedimento in Germania, sia pure relativamente al trattamento dei dati biometrici di una sola persona, il Sig. Matthias Marx (provvedimento del 27 gennaio 2021 dell'autorità per la protezione dei dati personali della città di Amburgo, su cui v. la notizia n. 8 nel numero 1/2021 di questa Rubrica http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf).

Clearview AI è una società statunitense, costituita nel 2017, che ha creato un motore di ricerca di immagini, all'interno di un proprio database, tramite riconoscimento facciale. A tal fine, la società raccoglie, attraverso tecniche di *web scraping*, immagini da social network, blog e siti web in cui sono presenti foto o video liberamente accessibili che vengono elaborati con tecniche biometriche al fine di estrarre le caratteristiche identificative del volto di ogni persona ritratta per consentirne l'indicizzazione e la successiva ricerca. Clearview ottiene così profili basati sui dati biometrici estratti dalle immagini, eventualmente arricchiti da altre informazioni ad esse correlate come titolo, geolocalizzazione della foto o pagina web di pubblicazione, consentendole di offrire un servizio di ricerca delle persone. La piattaforma è dichiaratamente stata creata al fine di fornire un servizio di ricerca biometrica altamente qualificata.

Diversamente da quanto affermato dalla società, che non si riteneva soggetta al GDPR (il Regolamento UE 2016/679, di seguito il "**Regolamento**") in quanto avente sede legale negli USA e perché dichiarava di non offrire i propri servizi a cittadini europei, il Garante ha accertato che la stessa ha invece trattato i dati anche di cittadini italiani e di persone collocate in Italia. Inoltre, mentre la società ha sostenuto di non tracciare né monitorare le persone nel tempo, ma di eseguire una forma di classificazione che si risolverebbe in un'istantanea dei risultati della ricerca al momento del compimento della stessa, il Garante ha constatato invece la realizzazione di una comparazione tra immagini idonea ad integrare un'attività assimilabile al controllo del

comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione.

Il Garante ha accertato inoltre l'illiceità del trattamento dei dati personali detenuti dalla società, inclusi quelli biometrici e di geolocalizzazione, in quanto effettuato senza un'adeguata base giuridica respingendo la tesi della difesa secondo la quale il trattamento si poteva basare sul legittimo interesse.

Secondo il Garante, la società ha poi violato altri principi del Regolamento come: quelli relativi agli obblighi di trasparenza, non avendo adeguatamente informato gli interessati; quello di limitazione delle finalità del trattamento, avendo utilizzato i dati per scopi diversi rispetto a quelli per i quali erano stati pubblicati online; e quello di limitazione della conservazione, non avendo stabilito tempi di conservazione dei dati.

Conseguentemente, il Garante ha rilevato la violazione degli artt. 5, par. 1, lett. a), b) ed e), 6, 9, 12, 13, 14, 15 e 27 del Regolamento e comminato una sanzione amministrativa di 20 milioni di euro oltre al divieto di prosecuzione del trattamento, l'ordine di cancellare i dati relativi a persone che si trovano in Italia, nonché quello di designare un rappresentante nel territorio dell'Unione europea che funga da interlocutore, in aggiunta o in sostituzione del titolare con sede negli Stati Uniti, al fine di agevolare l'esercizio dei diritti degli interessati.

GUIDO D'IPPOLITO

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

9. La decisione del 13 gennaio 2022 del garante privacy austriaco sul trasferimento di dati personali negli USA da parte di Google Analytics

Il 13 gennaio 2022 l'autorità garante per la protezione dei dati austriaca ("**Datenschutzbehörde**" o "**DSB**") si è pronunciata sulla legittimità dell'utilizzo di Google Analytics. La decisione deve essere letta alla luce della sentenza "Schrems II" con cui a luglio 2020 la Corte di Giustizia dell'UE aveva dichiarato illegittimo il *Privacy Shield* in quanto gli Stati Uniti non garantivano un livello di protezione dei dati personali equivalente a quello riconosciuto nell'UE dal GDPR (su cui v. la notizia n. 1 nel numero 3/2020 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf). In seguito alla decisione della Corte, ad agosto 2020, il gruppo Noyb - fondato dallo stesso Schrems - aveva presentato 101 reclami davanti alle autorità garanti di diversi Stati Membri contro società che trasferivano dati personali verso gli USA attraverso Google Analytics e/o Facebook Connect integrations.

L'autorità austriaca è stata la prima a pronunciarsi su uno di questi reclami con riferimento ad un sito web che trasferiva i dati degli utenti negli Stati Uniti attraverso l'utilizzo di Google Analytics. Il DSB ha ritenuto che il trattamento dei dati personali effettuato attraverso Google Analytics violi il Capo V del GDPR in quanto i dati personali sono trasferiti verso un Paese extra UE - gli USA - che non garantisce un livello di protezione equivalente a quello assicurato dalla normativa europea sulla protezione dei dati. Questo, in particolare, a causa della possibilità per le autorità statunitensi di accedere ai dati detenuti da Google e di identificare l'utente interessato. Anche l'uso di *Anonymize IP* (il servizio di Google Analytics che permette di rimuovere le prime cifre dell'indirizzo IP, rendendolo così non più associabile all'utente) è stato considerato dall'autorità irrilevante, in quanto l'indirizzo IP è solo "un pezzo del puzzle" e Google può utilizzare altri dati in suo possesso per riuscire ad individuare l'utente. Sia le Clausole Contrattuali Standard (di cui Google si è servita in seguito all'invalidamento del *Privacy Shield*) che le misure supplementari (contrattuali, organizzative e tecniche) adottate da Google per rendere il trasferimento dei dati conforme al GDPR sono state ritenute insufficienti. Infatti, a detta del DBS, qualsiasi misura supplementare può essere considerata efficace solo se affronta le carenze specifiche individuate nella valutazione della situazione nel paese terzo, vale a dire in questo caso le possibilità di accesso e di sorveglianza da parte dei servizi segreti statunitensi. Tuttavia, le misure contrattuali di per sé non hanno efficacia vincolante nei confronti delle autorità del paese terzo, per cui devono essere integrate con ulteriori misure. La stessa crittografia non è stata considerata una misura adeguata in quanto se il *provider* possiede la chiave (come nel caso di Google), in caso di richiesta di accesso da parte delle autorità statunitensi potrà essere obbligato a rivelare tale chiave insieme ai dati, vanificando così di fatto la relativa protezione.

Questa decisione avrà probabilmente un profondo impatto sul tema del trasferimento dei dati personali verso gli Stati Uniti che, dopo più di un anno dalla sentenza "Schrems II", non ha ancora

avuto sviluppi significativi. Nonostante l'annullamento del *Privacy Shield*, infatti, le società europee hanno di fatto continuano ad avvalersi di *provider* i cui *server* si trovano negli USA o che, comunque, sono soggetti alla legge statunitense. In particolare, Google Analytics rimane oggi la piattaforma di *web analytics* maggiormente utilizzata dai *website owner* e difficilmente sostituibile. D'altra parte, è evidente come il problema del trasferimento dei dati verso gli USA vada ben oltre i singoli titolari, nonché le stesse *big tech.* Si tratta, infatti, di un problema principalmente politico che richiede necessariamente una soluzione a monte attraverso il raggiungimento di un accordo tra la Commissione Europea e il Governo statunitense.

CHIARA RAUCCIO

https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf

10. La decisione del 10 febbraio 2022 del garante privacy francese sul trasferimento di dati personali negli USA da parte di Google Analytics

Dopo la pronuncia dell'autorità austriaca, anche l'autorità garante della protezione dei dati personali francese ("***Commission Nationale de l'Informatique et des Libertés***" o "**CNIL**") il 10 febbraio 2022 è intervenuta sul tema del trasferimento dei dati personali verso gli Stati Uniti attraverso Google Analytics. Anche in questo caso l'autorità si è pronunciata in seguito ad un reclamo presentato da Noyb (associazione fondata da Schrems) sulla base della sentenza "Schrems II" con cui a luglio 2020 la Corte di Giustizia dell'UE ha invalidato il *Privacy Shield*. La decisione del CNIL si pone sulla scia di quella adottata poco più di un mese prima dall'omologa autorità austriaca, confermando così l'atteggiamento unitario adottato dalle *Data Protection Authority* ("**DPA**") europee sul tema del trasferimento dei dati personali verso gli USA.

Il CNIL ha innanzitutto esaminato il funzionamento di Google Analytics e le modalità con cui avviene il trasferimento dei dati personali. Google Analytics – il servizio di *web analytics* ad oggi più utilizzato a livello globale - può essere integrato nei siti web per misurare in termini statistici il numero di utenti che visitano la pagina. Per fare ciò ad ogni visitatore viene associato un identificatore univoco. Tuttavia, nonostante l'analisi sia aggregata e l'identificatore sia tenuto separato dai dati identificativi dell'utente, l'identificatore costituisce comunque un dato personale in quanto Google, combinandolo con altri dati in suo possesso, rimane in grado di associarlo ad una persona fisica determinata.

Conseguentemente, il trasferimento verso gli Stati Uniti degli identificatori e delle informazioni relative alle interazioni degli utenti ad essi associati pone un tema di legittimità del trasferimento ai sensi della normativa UE in materia di protezione dei dati personali. Nello specifico il CNIL ha ribadito che, in seguito alla sentenza Schrems II e all'assenza di una nuova decisione di adeguatezza, il trasferimento dei dati verso gli USA può avvenire solo sulla base di adeguate garanzie. Tuttavia, secondo l'autorità francese – come del resto già sostenuto dall'autorità austriaca – le misure supplementari poste in essere da Google non sono sufficienti a garantire un livello di protezione adeguato. La *parent company* di Google (Alphabet Inc.), infatti, rientra tra gli operatori economici soggetti alle leggi di sorveglianza degli Stati Uniti, con la conseguenza che i servizi segreti statunitensi hanno *ex lege* la facoltà di accedere ai dati acquisiti tramite il servizio Analytics. Alla luce di ciò le misure di sicurezza adottate da Google, non avendo efficacia vincolante nei confronti delle autorità di sorveglianza statunitensi, non sono in grado di impedire l'accesso ai dati da parte dei servizi di *intelligence* e, dunque, non eliminano il rischio per gli utenti europei dei siti web che utilizzano il servizio. Ne consegue che il trasferimento ad oggi effettuato attraverso Google Analytics viola le disposizioni del Capo V del GDPR ed è, dunque, illegittimo.

Il CNIL non ha irrogato una sanzione al sito web oggetto del provvedimento, ma ha concesso un mese di tempo per porre fine alla violazione interrompendo l'utilizzo di Google Analytics, se necessario, o utilizzando un servizio che non implichi il trasferimento dei dati verso gli Stati Uniti. Al riguardo il CNIL ha raccomandato di utilizzare solo strumenti che producano dati statistici anonimi, così da evitare trasferimenti illegali, e ha avviato un piano di valutazione per determinare quali soluzioni sul mercato consentano di non raccogliere il consenso dell'interessato.

In ogni caso la decisione in esame risulta di particolare rilievo in quanto conferma la posizione intransigente assunta dalle DPA europee rispetto ai trasferimenti di dati verso gli Stati Uniti, evidenziando nuovamente l'esigenza sempre più pressante di una soluzione.

CHIARA RAUCCIO

https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

11. La decisione del 2 febbraio 2022 del garante privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe

Il 2 febbraio 2022 la *Litigation Chamber* del Garante per la protezione dei dati personali belga ("**Garante Privacy**" o "**Autorità**"), quale organo amministrativo di risoluzione delle controversie, ha dichiarato l'illegittimità dei trattamenti di dati su larga scala effettuati dalla *Interactive Advertising Bureau Europe* ("**IAB Europe**") in quanto violativi di numerose disposizioni del GDPR, comminando relative sanzioni, di seguito illustrate.

Nello specifico, l'oggetto del provvedimento è duplice, concernendo, *in primis*, la conformità al GDPR del *Transparency & Consent Framework* ("**TCF**") predisposto e gestito da IAB Europe e, conseguentemente, il suo impatto sul c.d. *Real-Time Bidding* ("**RTB**").

Il settore della pubblicità online opera "dietro le quinte" delle pagine web, attraverso metodi di c.d. *"Programmatic advertising"* tra cui primeggia l'offerta in tempo reale (RTB), definita in letteratura come rete di partner che permette applicazioni di *big data* per migliorare le vendite di spazi pubblicitari predeterminati attraverso il *marketing* guidato dai dati in tempo reale e la pubblicità (comportamentale) personalizzata. Si tratta, in sostanza, di un sistema di aste virtuali istantanee e automatizzate tramite algoritmi, attraverso cui si realizza l'interscambio di offerte d'acquisto di spazi pubblicitari personalizzati. Come minutamente illustrato dall'Autorità, il RTB coinvolge: *i*) le imprese che gestiscono il sistema e ne delineano le politiche, la *governance* e i protocolli tecnici; *ii*) dal lato dell'offerta, le imprese che possiedono siti web o applicazioni con disponibilità di spazi pubblicitari ("*publishers*") e quelle che gestiscono piattaforme online automatizzate sulle quali i *publishers* registrati possono segnalare la disponibilità dei propri spazi pubblicitari, sollecitandone la domanda ("*Sell-Side Platforms"* o "SSP"); *iii*) dal lato della domanda, gli inserzionisti e le imprese che gestiscono piattaforme di ottimizzazione della richiesta di spazi pubblicitari (*"Demand-Side Platforms"* o "DSPs"); *iv*) intermediari che veicolano gli scambi, vieppiù consentendo alle DSP di emettere offerte parametrate sulle richieste avanzate dalle SSP (*"Ad Exchanges"*); *v*) le cc.dd. "*Data Management Platforms"* ("DMP"), che estraggono ingenti quantità di dati personali di vario tipo da molteplici fonti (dispositivi, *cookies*, identificatori mobili, analisi comportamentali, *social media*, dati offline ecc.), per poi centralizzarli, analizzarli e classificarli mediante algoritmi, fornendo così profili dettagliati dei consumatori per l'ottimizzazione del *targeting* e la personalizzazione delle offerte. La dinamica è, in estrema sintesi, la seguente: dopo aver elaborato profili dettagliati di consumatori tramite una DMP, gli inserzionisti emettono offerte tramite le DSP per intercettare la disponibilità dei pertinenti spazi pubblicitari dei *publishers* segnalati via SSP; perciò, non appena l'utente accede a una pagina web: i *publishers* interessati selezionano una SSP; questa seleziona un *Ad exchange*; esso invia richieste di offerte a centinaia di partner della rete, invitandoli a rispondere, e piazza l'offerta maggiore; infine, la DSP presenta l'annuncio dell'inserzionista vincitore.

Così delineato, il RTB, anche per dimensione e numero di operatori coinvolti, presenta rischi seri e fisiologici, tra cui: la profilazione e il processo decisionale automatizzato; il trattamento su larga scala anche di categorie speciali di dati, uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative; abbinamento o fusione di *datasets*; analisi o previsione del comportamento, della posizione o dei movimenti delle persone fisiche; trattamenti non trasparenti.

Fra i protocolli maggiormente utilizzati a livello mondiale per il RTB vi sono il sistema "OpenRTB", assieme all'associato *"Advertising Common Object Model"* (AdCOM), sviluppati da IAB *Technology Laboratory Inc.* ("IAB Tech Lab") e *Interactive Advertising Bureau Inc*. ("IAB"), e il sistema di "acquirenti autorizzati" "AdBuyers", sviluppato da Google. Entità affatto distinta è IAB Europe, federazione rappresentativa di circa 5000 imprese e associazioni nazionali operanti nel ramo della pubblicità e del marketing digitale, cui si deve la paternità del TCF, ossia l'insieme di politiche, specifiche tecniche, termini e condizioni proposte come standard di *best practice* intersettoriale asseritamente idoneo ad assicurare la conformità dell'industria della pubblicità digitale con la regolazione UE in materia di protezione dei dati personali. Perciò, ferma la distinzione ontologica tra TCF e OpenRTB, essi sono fatalmente destinati a intersecarsi, giacché – come affermato da IAB Europe – il primo fornisce un quadro operativo di allineamento al GDPR dei trattamenti svolti sulla base del secondo. Inoltre, se vi è larga coincidenza fra gli attori dei due sistemi, una peculiarità del TCF è la presenza delle cc.dd. *"Consent Management*

Platforms" ("CMPs"), consistenti in *pop-up* mostrati all'atto della prima connessione a un sito web per raccogliere il consenso dell'utente al posizionamento di *cookie* e altre informazioni identificative. Ebbene, parte essenziale dell'intervento delle CMP è la generazione di una stringa composta da una combinazione di lettere, numeri e altri caratteri, denominata "*Transparency and Consent String*" ("TC *String*"), volta all'acquisizione automatica di preferenze dell'utente quali: il consenso o meno al trattamento dei dati personali per scopi di *marketing* o altri, la condivisione o meno dei dati con terze parti venditori e l'esercizio o meno del diritto di opposizione. In estrema sintesi, la TC *String* viene decifrata dai cc.dd. *"Adtech vendors"* (inserzionisti, SSP, DSP, *Ad Exchanges* e DMP) per determinare la sussistenza della base giuridica necessaria a trattare i dati personali di un utente.

Ciò premesso, l'esame della *Litigation Chamber* ha ad oggetto esclusivamente il trattamento di dati personali all'interno del TCF e le relative responsabilità, affrontando solo *per incidens* le attività compiute nel sistema OpenRTB e i relativi rischi.

Anzitutto, l'Autorità dichiara che le preferenze degli utenti raccolte nella TC String costituiscono tecnicamente dati personali. Infatti, tanto la legislazione UE (cfr. art. 4, paragrafo 1 GDPR e art. 2.a Convenzione di Strasburgo del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale) quanto la giurisprudenza della CGUE adottano un concetto ampio di dato personale, al fine di garantire un elevato livello di tutela degli interessati. Costituisce dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o (indirettamente) per mezzo di identificatori ai quali l'utente può essere collegato attraverso i suoi dispositivi, applicazioni, strumenti e protocolli, come gli indirizzi IP, i *cookie* di identificazione o altri (cfr. considerando n. 30 GDPR). In altri termini, ove determinate informazioni possono essere associate a una persona identificata o identificabile tramite i mezzi che possono ragionevolmente impiegarsi, esse devono qualificarsi come dati personali. Ebbene, nonostante sia pacifico che la TC String, a ragione della limitatezza e del carattere delle informazioni *ivi* contenute, non consente un'identificazione diretta dell'interessato, quest'ultimo è certamente identificabile. Infatti, i *pop-up* di consenso predisposti e gestiti dalle CMP elaborano inevitabilmente anche l'indirizzo IP dell'utente, il quale diviene così agilmente associabile alle preferenze raccolte nella stringa memorizzata o letta dalla stessa CMP. In sostanza, è proprio la possibilità di associare le TC String agli indirizzi IP a rendere identificabile l'interessato. Ne consegue non solo che IAB Europe dispone di mezzi ragionevoli per l'identificazione degli utenti ma financo che ciò, a ben vedere, parrebbe essere lo scopo ultimo delle operazioni effettuate nell'ambito del *framework*. Una volta chiarita la natura di dati personali delle preferenze degli interessati, deve concludersi anche che il quadro del TCF presuppone fisiologicamente il trattamento degli stessi ai sensi dell'art. 4.2. GDPR, ponendosi come approccio standardizzato per la raccolta, l'elaborazione, l'archiviazione e la successiva condivisione delle preferenze degli utenti.

Ai fini dell'attribuzione di responsabilità in capo a IAB Europe, questione preliminare è poi la sua qualificabilità come titolare del trattamento *ex* art. 4.7 GDPR. Anche tale nozione è piuttosto ampia, al precipuo scopo di ricomprendervi le entità che esercitano un controllo effettivo sulle operazioni di trattamento, determinandone, singolarmente o insieme ad altri, le finalità e i mezzi. Inoltre, come chiarito dal Comitato europeo per la protezione dei dati (lo "**EDPB**"), tale influenza può esercitarsi anche tramite poteri impliciti o di fatto. In quest'ottica, diviene cruciale il ruolo funzionale che un operatore assume: dalla giurisprudenza si apprende infatti che non è necessario un accesso diretto ai dati personali né tantomeno che il trattamento sia effettuato in prima persona, essendo sufficiente l'esercizio di un'influenza decisiva sul "perché" e sul "come" di tali operazioni. Il TCF, beninteso, non integra di per sé un trattamento; e tuttavia, come *supra* illustrato, esso integra un quadro di politiche e specifiche tecniche vincolanti nel cui contesto i trattamenti si strutturano di fatto sulle linee elaborate da IAB Europe. In particolare, l'accettazione dei *Terms and Conditions* da parte degli *Adtech vendors* obbliga quest'ultimi a osservare regole predefinite per il trattamento delle TC String nel TCF. In quest'ottica, dalla documentazione redatta da IAB Europe emerge anzitutto che gli scopi della TC String e, *amplius*, del suo trattamento nell'ambito del TCF sono determinati puntualmente da IAB Europe mediante un elenco tassativo. Inoltre, quest'ultima individua e prescrive anche i mezzi essenziali – quelli cioè strettamente legati allo scopo e alla portata del trattamento (cfr. EDPB - *Guidelines 7/2020 on the concepts of controller and processor in the GDPR*, v2.0, 2021, par. 39-41) – per l'elaborazione della TC String. Ad esempio, le politiche, le specifiche tecniche e le linee guida di attuazione del TCF precisano che le CMP, nel raccogliere il consenso degli utenti, debbano

generare una stringa unica e memorizzarne il valore. Per far ciò, sono obbligati a registrarsi presso IAB Europe e a seguire le specifiche tecniche, sviluppate in collaborazione con IAB Tech Lab, attinenti all'API132, con cui la stringa può essere generata e letta da *publishers* e *Adtech vendors*. Le medesime regole ne individuano altresì il contenuto, specificando le informazioni incluse. In generale, IAB Europe determina di fatto le modalità di generazione, conservazione e condivisione della TC String, con cui vengono trattate le preferenze, le obiezioni e il consenso degli utenti. Ne consegue che IAB Europe deve senz'altro qualificarsi come titolare del trattamento ai sensi dell'art. 4, paragrafo 7 GDPR.

Per inciso, quanto sopra non implica che la titolarità dei trattamenti, e la conseguente responsabilità, sia esclusivamente di IAB Europe. All'opposto, l'Autorità ritiene configurabile un'ipotesi di contitolarità *ex* art. 26 GDPR con le CMP, i *publishers* e gli *Adtech vendors*, avendosi di fatto una determinazione congiunta delle finalità e dei mezzi. Naturalmente, la misura delle responsabilità individuali è variabile in base alla concreta entità e alla fase di coinvolgimento del singolo attore, essendo necessaria solamente una convergenza di decisioni in modo che ne sia provata una tangibile mutua influenza. Al riguardo, a ben vedere, IAB Europe realizza, col TCF, un sistema all'interno del quale il consenso, le obiezioni e le preferenze degli utenti sono raccolti e scambiati non per i propri scopi o per la propria conservazione, bensì per agevolare l'ulteriore trattamento da parte di terzi qualificati.

Passando all'esame delle violazioni del GDPR, l'Autorità muove dalla liceità e correttezza del trattamento. Ai fini della verifica di compatibilità con gli artt. 5, paragrafo 1 e 6 GDPR, vengono distinte preliminarmente: *a*) le attività di acquisizione del consenso, delle obiezioni e delle preferenze degli utenti nella TC String da parte delle CMP; *b*) la raccolta e la diffusione dei dati personali degli utenti nel protocollo OpenRTB da parte delle imprese partecipanti al TCF.

Ferma la qualificabilità delle operazioni di generazione e diffusione della TC String come trattamenti di dati, se ne indaga dunque la base giuridica. Né le politiche né le linee guida del TCF prevedono un obbligo per le CMP di ottenere il consenso inequivocabile degli utenti prima di acquisire le loro preferenze nella stringa. A ciò si accompagna un rilevante difetto di informazione, poiché l'utenza non è posta a conoscenza dell'esistenza stessa dei trattamenti, dei soggetti con cui vengono condivise le loro preferenze, né i tempi di conservazione delle stesse: l'art. 6, lett. *a*) GDPR non è quindi applicabile. Del pari, non è invocabile la lett. *b*), difettando il requisito dell'obiettiva necessità del trattamento alla fornitura di servizi online da parte dei *publishers* agli utenti interessati, sempre ammesso che sussista a monte un effettivo rapporto contrattuale. Per tali ragioni, l'analisi si incentra sull'art. 6, lett. *f*), ossia sulla sussistenza di un interesse legittimo del titolare del trattamento o di terzi, debitamente bilanciato con gli interessi o i diritti e le libertà fondamentali degli interessati. Com'è noto, il requisito *de quo* richiede il cumulo di tre condizioni analiticamente indicate dalla giurisprudenza della CGUE (sentenza Rigas, 11 dicembre 2009, C-708/18), dovendosi dimostrare che: gli interessi perseguiti col trattamento siano riconosciuti come legittimi (*"test dello scopo"*); che il trattamento sia necessario per il perseguimento dell'interesse legittimo (*"test di necessità"*); non siano lesi diritti e libertà fondamentali dell'interessato (*"test del bilanciamento"*). Ebbene, la *Litigation Chamber* ritiene che le prime due verifiche abbiano esito positivo, dal momento che l'acquisizione del consenso e delle preferenze degli utenti, come parte essenziale del TCF, integra un interesse legittimo di IAB Europe e degli *Adtech vendors* coinvolti e i dati personali inclusi nella TC String sono limitati a quanto strettamente necessario a tale scopo. Per quanto concerne il terzo test, il considerando n. 47 GDPR impone che il bilanciamento tenga conto delle ragionevoli aspettative degli interessati, dovendosi valutare se questi, al momento e nel conteso concreto in cui avviene la raccolta dei dati, potevano prefigurarsi un trattamento degli stessi per il perseguimento dell'interesse legittimo debitamente esplicitato *ex* art. 5, lett. *b*) GDPR. Il quadro fattuale dimostra l'assenza di possibilità per gli utenti di opporsi *in toto* ai trattamenti effettuati nel contesto del TCF, essendo automatica la generazione della stringa da parte delle CMP e il suo collegamento all'ID unico dei singoli interessati attraverso un *cookie euconsent-v2* posto sui loro dispositivi. L'esito negativo del *balancing test* impedisce dunque l'invocabilità dell'art. 6, lett. *f*), da cui discende fatalmente la declaratoria di violazione degli artt. 5, paragrafo1 e 6 GDPR per mancanza di una valida base giuridica dei trattamenti condotti nell'ambito del TCF.

Per quanto concerne la raccolta e la diffusione dei dati personali degli utenti nel contesto del protocollo OpenRTB da parte delle imprese partecipanti al TCF, la base giuridica di tali operazioni non può ritenersi offerta dall'art. 6, lett. *a*), poiché il consenso ottenuto dalle CMP non soddisfa i requisiti dell'art. 7 GDPR. Esso, infatti, non risulta sufficientemente libero, specifico,

informato e non ambiguo. Anzitutto, alcune le finalità di trattamento indicate da IAB Europe nelle politiche del *framework*, come la "misurazione della performance dei contenuti" o la "applicazione di ricerche di mercato per generare previsioni sul pubblico", sono intrasparenti e financo decettive, non fornendo informazioni sull'ambito del trattamento, sulla natura dei dati i trattati o sulle tempistiche di conservazione. Inoltre: l'interfaccia utente delle CMP non fornisce una panoramica delle categorie di dati raccolti; risulta particolarmente ostico per gli utenti ottenere maggiori informazioni sull'identità dei soggetti coinvolti come contitolari dei trattamenti, difficoltà acuita dall'ingente numero di attori, che rende di fatto impossibile un consenso realmente informato; infine, il consenso, una volta ottenuto dalle CMP, non può essere ritirato dagli utenti con la stessa facilità con cui è prestato, non avendosi alcuna misura per impedire agli *Adtech vendors* di proseguire le operazioni avviate sulla base del consenso inziale. Ciò chiarito, il *focus* non può che spostarsi sull'art. 6, lett. *f*), indagando se e fino a che punto possa intravedersi un legittimo interesse a fondamento del *target advertising* e della profilazione. In questo caso, il triplice test rivela un esito ancor più negativo. Difatti, la genericità delle finalità di trattamento rende ardua la valutazione di necessità delle menzionate operazioni, non consentendo di rinvenire una base giuridica sufficientemente specifica, esistente, attuale e non ipotetica. A ben vedere, infatti, le politiche TCF non contemplano un obbligo per le CMP di esplicitare i legittimi interessi, prescrivendo requisiti specifici per l'interfaccia utente (UI) circoscritti a un livello meramente secondario di informazioni. Non solo. Nonostante si discorra di requisiti minimi, il TCF dispone che l'UI contenga esclusivo riferimento alle definizioni degli scopi pubblicati nel testo legale standard, cui è attribuito carattere "definitivo". Perciò, l'interpretazione della *Litigation Chamber* è nel senso che tali regole proibiscono di fatto alle CMP di fornire ulteriori informazioni agli interessati tanto in merito agli interessi legittimi perseguiti quanto al bilanciamento con i diritti e le libertà fondamentali dell'utente. In sostanza, dunque, il test dello scopo non può dirsi superato. Analogamente deve dirsi per il test di necessità, mancando adeguate garanzie che i dati raccolti e diffusi siano limitati a quanto strettamente necessario per le finalità previste. Infine, l'elevato numero di attori operanti nel TCF non consente agli interessati di sviluppare ragionevoli aspettative ai sensi del considerando n. 47 GDPR, dovendo escludersi un acconcio bilanciamento. Per completezza, si aggiunge che il TCF non contempla, per le ipotesi in questione, alcun riferimento alla necessità contrattuale come base giuridica *ex* art. 6, lett. *b*) GDPR.

L'esame in merito alle asserite violazioni del GDPR prosegue con riferimento ai presidi di trasparenza prescritti agli artt. 12, 13 e 14 del regolamento. In proposito, si rileva preliminarmente come le politiche del TCF attribuiscano in certi casi a IAB Europe il potere di reclamare le registrazioni del consenso che le CMP sono tenuti a conservare, omettendo però di prevedere un correlativo obbligo di informazione circa tale possibile trattamento. Ma soprattutto, il numero di *Adtech vendors* potenzialmente coinvolti nel ricevere e trattare ulteriormente i dati degli utenti sulla base delle preferenze da essi prestate, unita all'echeggiata genericità di alcune delle finalità dichiarate, non consente di ritenere soddisfatto il requisito di una forma trasparente, intellegibile e facilmente accessibile di cui all'art. 12.1 GDPR, con particolare enfasi sulla grave assenza di quell'elemento di concisione sul quale già il "Gruppo 29" insisteva per evitare un "affaticamento informativo" (WP 260 – *Guidance on transparency under the GDPR*, par. 8). Per tali ragioni, l'Autorità ritiene che il TCF violi le condizioni di trasparenza richieste dagli artt. 12, 13 e 14 GDPR.

Infine, è analizzata la compatibilità del quadro TCF con i principi di responsabilità (art. 24 GDPR), protezione dei dati fin dalla progettazione e per impostazione definita (Art. 25 GDPR), integrità e riservatezza (art. 5.1 GDPR) e sicurezza nel trattamento (art. 32 GDPR). Com'è noto, l'art. 24 impone al titolare del trattamento di approntare misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (con obbligo di riesame e aggiornamento), in ciò riflettendo l'art. 5.2. Inoltre, in consonanza col considerando n. 74, le misure *de quibus* devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Ai sensi dell'art. 32, poi, il titolare e il responsabile devono mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza del trattamento adeguato al rischio. Si tratta di un punto di grande importanza, che si lega a doppio filo coi principi di integrità e riservatezza e i conseguenti obblighi di sicurezza dei dati e di protezione mediante misure tecniche e organizzative adeguate di cui all'art. 5, lett. *f*). Infatti, in assenza di opportuni presidi in tal senso, spiega l'Autorità, il rispetto dei diritti fondamentali

non può essere efficacemente assicurato, vieppiù in considerazione del ruolo cruciale svolto dalle tecnologie dell'informazione e della comunicazione nella nostra società. In altri termini, dato l'altissimo numero di TC String generate quotidianamente in seno al TCF, è essenziale che le norme che ne regolano la partecipazione siano osservate da tutte le parti coinvolte e che tale osservanza sia supervisionata da IAB Europe in qualità di *"Managing Organisation"*. Tuttavia, sono le stesse politiche redatte da IAB Europe a prendere in considerazione l'ipotesi che, difettando un sistema di convalida, le CMP possano falsificare o modificare le TC String e, precisamente, i segnali generativi del *cookie euconsent-v2*, riproducendo consensi "falsi", non effettivamente (o comunque, non validamente) prestati dagli interessati. Che le misure di controllo offerte nel TCF siano insufficienti lo rivela anche il c.d. *"TCF Vendor Compliance Programme"*, ove, a fronte di declamatori incoraggiamenti a garantire la sicurezza dei trattamenti, difetta un monitoraggio sistematico da parte di IAB Europe. Infine, il citato programma contempla un sistema sanzionatorio scarsamente dissuasivo, potendo, ad esempio, un venditore dichiararsi responsabile di una violazione fino a tre volte, prima di ricevere un termine di ventotto giorni per conformarsi, alla scadenza del quale sarà rimosso (peraltro non irreversibilmente) dalla *Global Vendors List*. In conclusione, dunque, la *Litigation Chamber* ascrive in capo a IAB Europe una responsabilità per violazione dell'obbligo di garantire la sicurezza, l'integrità e la riservatezza dei trattamenti.

Per completezza, si compendiano alcuni rilievi finali in merito ad ulteriori asserite violazioni del GDPR. *In primis*, la limitata entità dei dati sul singolo utente memorizzati nelle TC String porta a escludere una violazione dei principi di limitazione delle finalità e di minimizzazione dei dati (art. 5, lett. *b*) e *c*) GDPR) nel contesto della TCF, potendosi quest'ultima verificare solo in seno al protocollo OpenRTB, rispetto al quale però IAB Europe non agisce come titolare dei trattamenti. Inoltre, non è provata la conservazione delle TC String e la relativa memorizzazione dei dati personali per periodi di tempo non autorizzati, in violazione dell'articolo 5, lett. *e*) GDPR. Di particolare importanza è il rilievo che le TC String non contengono in sé informazioni tali da poter estrarre – neanche indirettamente, rendendo ad esempio accessibile la cronologia dei siti web visitati dall'interessato – categorie particolari di dati personali *ex* art. 9 GDPR. Risultano invece violati: l'art. 30 GDPR sulla tenuta dei registri delle attività di trattamento, per mancanza di riferimenti ai segnali di consenso, alle obiezioni e alle preferenze degli utenti; l'obbligo di effettuare la valutazione di impatto sulla protezione dei dati *ex* art. 35; l'obbligo di nominare un DPO ai sensi dell'art. 37.

In considerazione dei suesposti rilievi, l'Autorità, al fine di rendere il trattamento dei dati personali nell'ambito del TCF conforme alle disposizioni del GDPR, adotta gli ordini di conformità, i divieti e commina le sanzioni che seguono. A IAB Europe è ordinato di: fornire una base giuridica valida per il trattamento e la diffusione delle preferenze degli utenti sotto forma di TC String e di un *cookie euconsent-v2*, vietando al contempo il ricorso a interessi legittimi; assicurare misure di controllo tecniche e organizzative efficaci per garantire l'integrità e la riservatezza della TC String, in conformità con gli artt. 5.1., lett. *f*), 24, 25 e 32 GDPR; mantenere un audit rigoroso delle organizzazioni partecipanti al TCF; adottare misure tecniche e organizzative per evitare che il consenso sia prestato di default nelle interfacce delle CMP e per impedire l'autorizzazione automatica dei fornitori partecipanti che fondano su interessi legittimi i loro trattamenti, in conformità con gli artt. 24 e 25 GDPR; costringere le CMP ad adottare un approccio uniforme e conforme al GDPR per le informative prestata agli utenti, in conformità con gli artt. 12, 13, 14 e 24 GDPR; aggiornare i registri dei trattamenti, includendo il trattamento dei dati personali nel TCF da parte di IAB Europe, in conformità con l'art. 30 GDPR; effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) sui trattamenti operati nell'ambito del TCF e sul loro impatto sulle attività effettuate nel sistema OpenRTB, con i dovuti riesami in caso di versioni future o modifiche al TCF, conformemente all'articolo del 35 GDPR; nominare un responsabile della protezione dei dati (DPO) in conformità agli artt. 37-39 GDPR. Per il completamento di tali misure è assegnato a IAB Europe un termine massimo di sei mesi dalla convalida di un piano d'azione da parte dell'Autorità, assistito da una penalità di € 5000 per ogni giorno di mancato adempimento. Infine, è comminata a IAB Europe una sanzione amministrativa di € 250.000 ai sensi dell'art. 83, paragrafo 5 GDPR.

VALENTINO RAVAGNANI

https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf

12. La sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie cache

Con la sentenza n. 3952/2022 dell'8 febbraio 2022, la Corte di Cassazione ha accolto parzialmente il ricorso proposto dalle società Yahoo! EMEA Ltd. e Yahoo! Italia S.r.l. in liquidazione (di seguito collettivamente "**Yahoo!**") avverso la sentenza del Tribunale di Milano n. 12623/2016, precisando che la richiesta di cancellazione delle copie *cache* relative alle informazioni accessibili tramite un motore di ricerca non può semplicemente accogliersi ogni qual volta sia stato stabilito il diritto alla deindicizzazione, bensì richiede una specifica ponderazione di bilanciamento tra il diritto all'oblio dell'interessato e il diritto del pubblico alla diffusione e alla acquisizione di informazioni relative ai fatti nel loro complesso, attraverso parole chiave anche diverse dal nome della persona.
Nel caso di specie, l'interessato aveva inoltrato al motore di ricerca Yahoo! una richiesta di rimozione dai risultati delle ricerche in Europa di diversi e specifici URL che collegavano il suo nome ad una vicenda giudiziaria da egli ritenuta non più rilevante per il diritto di cronaca (cd. deindicizzazione).
Yahoo! aveva dichiarato di non poter dare riscontro a tale richiesta, ritenendo di non essere qualificabile come titolare di tale trattamento di dati personali. Pertanto, l'interessato aveva depositato un ricorso presso il Garante per la Protezione dei Dati Personali (il "**Garante**"), con le richieste di rimozione degli URL nonché di cancellazione delle copie *cache* dalle pagine web accessibili tramite predetti URL.
Con provvedimento del 25 febbraio 2016, il Garante accoglieva parzialmente le richieste dell'interessato, ingiungendo a Yahoo! di rimuovere gli URL e di cancellare le copie *cache*, pronunciando invece non luogo a provvedere con riferimento ad altre richieste non più rilevanti.
Yahoo! domandava quindi al Tribunale di Milano l'annullamento del provvedimento del Garante. Il Tribunale di Milano confermava il contenuto del provvedimento impugnato e respingeva il ricorso, in quanto riteneva - in primo luogo, in merito alla rimozione degli URL - che sia l'interesse economico delle società e sia l'interesse della collettività a conoscere le informazioni derivanti dalla ricerca riferita al nome dell'interessato, siano in subordine rispetto ai diritti fondamentali dell'interessato stesso e - in secondo luogo, in merito alla cancellazione delle copie *cache* - che il provvedimento del Garante della Privacy fosse in linea con i principi ispiratori del GDPR (Regolamento UE 2016/679), pur pacificamente non applicabile al caso *ratione temporis*, in particolare quanto alla previsione del diritto ad una cancellazione estesa dei dati personali oggetto del trattamento.
Yahoo! impugnava (per cinque motivi) la decisione del giudice di merito dinanzi alla Corte di Cassazione.
La Corte ha rigettato i primi quattro motivi di ricorso confermando la competenza del Garante di emettere i provvedimenti nei confronti di Yahoo!, ai sensi dell'Articolo 7 del d.lgs. 196/2003, l'applicabilità del diritto italiano al caso di specie perché Yahoo! svolge un'attività effettiva e reale nel territorio italiano (sul punto, cfr. anche Corte di Giustizia dell'UE (Terza Sezione), Weltimmo s.r.o. contro Nemzeti Adatvédelmi és Információszabadság Hatóság, causa C-230/14, sentenza del 1° ottobre 2015, par. 41), e la legittimazione passiva della stessa Yahoo!.
Con il quinto motivo di ricorso, la ricorrente criticava, fra l'altro, un'interpretazione del diritto all'oblio sbilanciata in favore dell'interessato (in particolare, "la cancellazione delle copie *cache* delle pagine web accessibili attraverso gli URL"), a detrimento di interessi diversi, come l'interesse dei terzi di accedere alle pagine web per finalità diverse da quelle di una verifica sulle vicende giudiziarie dell'interessato.
Gli ermellini hanno preso in esame sia la rimozione degli URL sia l'eliminazione delle copie *cache*, richiamando i propri precedenti sulle tre nozioni del diritto all'oblio, del diritto alla cancellazione dei dati personali e del diritto alla deindicizzazione.
In particolare, nella sentenza in commento, si ricorda come le Sezioni Unite hanno ricondotto la deindicizzazione nell'ambito del diritto alla cancellazione dei dati, nel quadro della classificazione che considera lo stesso come una delle tre possibili declinazioni del diritto all'oblio, mentre le altre due, sono da individuare nel diritto a non vedere pubblicate nuovamente delle notizie relative a vicende legittimamente diffuse in passato, qualora sia trascorso un congruo periodo di tempo tra la prima e la seconda pubblicazione; ed infine, come esigenza a collocare la pubblicazione, legittimamente avvenuta molto tempo prima, nel contesto attuale (si veda Cassazione, Sezioni Unite, 22 luglio 2019, n. 19681).
La deindicizzazione è strumentale alla tutela giuridica dell'identità digitale dell'interessato e può essere un rimedio per impedire che i dati dell'interessato siano associati dal motore di ricerca ai fatti conservati in rete, venendo incontro al diritto delle persone a non essere trovati facilmente sulla rete.

Nel caso di specie, come già anticipato, la questione specifica affrontata dalla Corte di Cassazione non consisteva nella valutazione di legittimità o meno della deindicizzazione (ossia nel riconoscimento del "*right not to be found easily*"), bensì sulla parte della sentenza impugnata in cui il giudice di merito meneghino ha ritenuto corretto il provvedimento del Garante anche in merito alla cancellazione delle copie *cache* delle pagine web accessibili attraverso gli URL.

Sul punto, la Corte, dopo aver richiamato i principali risultati dell'elaborazione teorica sul diritto all'oblio, i punti 8 e 9 delle Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del GDPR adottate il 7 luglio 2020 dal Comitato Europeo per la Protezione dei Dati (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_it) e le importanti sentenze del medesimo giudice di legittimità Cass. n. 7559/2020 e Cass. 9147/2020, ha precisato che la cancellazione delle copie *cache*:

1. impedirebbe al motore di ricerca, nell'immediato, di utilizzare le stesse per indicizzare i contenuti per mezzo di parole chiave anche diverse da quella del nome dell'interessato;
2. farebbe sì che il motore di ricerca non potrebbe utilizzare nuove copie *cache* equivalenti a quelle oggetto del provvedimento del Garante che verrebbe, di conseguenza, ad assumere il contenuto di ingiunzione dinamica estendendosi a tutte le copie - con contenuto simile a quelle cui si riferisce il provvedimento - che il motore di ricerca possa realizzare nel futuro.

La valutazione che fa la Corte di Cassazione è che risulta necessario valutare non soltanto il diritto dell'interessato a dissociare l'informazione dal motore di ricerca attraverso l'interrogazione con il suo nome, ma anche l'interesse della collettività a poter trovare quella informazione tramite altri criteri di ricerca, in particolare per mezzo di parole chiave diverse dal nome della persona interessata.

Secondo gli ermellini, la cancellazione delle copie *cache* delle pagine accessibili dalle URL deve tenere conto di una specifica indagine circa il bilanciamento tra l'interesse del singolo ad essere dimenticato e l'interesse della collettività ad essere informata: il giudice di merito ha preso in considerazione solamente l'ambito dell'interessato, relativamente alla concessa indicizzazione, non valutando in maniera adeguata e specifica, quanto alla richiesta della cancellazione delle copie *cache*, l'interesse da parte della collettività ad essere informata sui fatti di cronaca nel suo complesso.

In conclusione, e su questa base, la Corte di Cassazione ha enunciato il seguente principio, rinviando al Tribunale di Milano, in diversa composizione, per farne applicazione: "la cancellazione delle copie *cache* relative a una informazione accessibile attraverso il motore di ricerca, in quanto incidente sulla capacità, da parte del detto motore di ricerca, di fornire una risposta all'interrogazione posta dall'utente attraverso una o più parole chiave, non consegue alla constatazione della sussistenza delle condizioni per la deindicizzazione del dato a partire dal nome della persona, ma esige una ponderazione del diritto all'oblio dell'interessato col diritto avente ad oggetto la diffusione e l'acquisizione dell'informazione, relativa al fatto nel suo complesso, attraverso parole chiave anche diverse dal nome della persona".

FRANCESCO GROSSI

https://web.uniroma1.it/deap/sites/default/files/allegati/Cass.-Civ.-Sez.-I-8-febbraio-2022-n.-3952.pdf

13. Le "Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration" dello European Law Institute (ELI) del 3 marzo 2022

Il 3 marzo 2022 lo *European Law Institute* di Vienna (in breve ELI) ha pubblicato un corposo documento che contiene regole generali sul procedimento diretto a valutare l'impatto («*Impact Assessment*») dei sistemi decisionali basati su algoritmi nella pubblica amministrazione.

Si tratta di un documento programmatico (e non vincolante), adottato sull'esempio di altre proposte redazionali elaborate da altri enti non istituzionali europei (si pensi alle *Model Rules on EU Administrative Procedure* del *Research Network on EU Administrative Law* – ReNEUAL), allo scopo di supportare future legislazioni dell'Unione, dei suoi Stati membri o di altri paesi extracomunitari (così espressamente a p. 12 del documento: «*the Model Rules are intended to be more general and adaptable in different legal contexts within and beyond the EU*») che intendano normare l'uso di sistemi decisionali algoritmici nel settore pubblico (art. 1, par. 1).

Secondo il documento dell'ELI, le decisioni amministrative algoritmiche si possono suddividere in due distinte tipologie: quelle "piene" in cui il processo formativo della volontà pubblica è completamente automatizzato; e quella "semipiene" in cui vi è spazio per la partecipazione umana nel

procedimento amministrativo informatico (art. 2, par. 1).

La metodologia operativa suggerita dal documento per soppesare adeguatamente la possibilità di usare algoritmi decisionali nel settore pubblico (al posto o in parziale sostituzione dell'intervento umano) è, come detto, la valutazione d'impatto; la quale, nelle intenzioni dell'ELI, dovrebbe assicurare a ogni amministrazione interessata (e quindi alla cittadinanza) la sicurezza, la completezza, la trasparenza, l'accessibilità e la responsabilità della soluzione organizzativa prescelta.

Scendendo nel dettaglio, il documento dell'ELI è composto da cinque capitoli suddivisi in sedici articoli e quattro allegati.

Esso parte dal presupposto che l'uso di sistemi algoritmici nella pubblica amministrazione non può seguire un unico approccio operativo («*precludes a one-size fits all approach*»; così si legge a p. 11), ma va opportunamente calibrato al contesto e all'ente di riferimento (la «*Implementing Authority*» secondo la dizione dell'art. 2, par. 2, n. 7).

Distingue perciò tra sistemi ad "alto rischio" (ossia a più elevato impatto sociale come l'ambiente, le telecomunicazioni, il fisco, le infrastrutture) per i quali è sempre consigliata una valutazione d'impatto rafforzata (allegato 1); sistemi a "basso rischio" (dove le criticità sono ben note e facilmente gestibili per legge) che ne sono esentati (allegato 2); sistemi a "medio rischio" per cui è richiesta una verifica d'impatto semplificata (art. 4); sistemi "incerti" e soggetti, in quanto tali, a una verifica preliminare per accertare in quale delle tre categorie principali rientrano (allegato 3).

In caso di valutazione d'impatto semplice (e sempre che non ricorrano particolari motivi di celerità o emergenza menzionati espressamente all'art. 1, par. 4 del documento dell'ELI) la procedura da seguire prevede la redazione di un piano d'azione (art. 6), anche col supporto di enti specializzati (art. 5), che deve contenere chiare ed esaustive informazioni: a) sul tipo di algoritmo che l'amministrazione procedente intenderà usare, sulle sue caratteristiche tecniche, sul suo modo di funzionamento, sulle finalità che esso vuole conseguire; b) sulla tutela dei diritti dei privati, sulle ricadute sociali, sui benefici della scelta organizzativa dell'amministrazione procedente; c) sulla sicurezza, tracciabilità, legalità e proporzionalità delle future decisioni prese dall'algoritmo; d) sulle garanzie tecniche fornite dal produttore del sistema informatico acquistato dall'amministrazione (art. 7); e) sulla protezione dei dati personali e della proprietà intellettuale (art. 8). Il documento così elaborato dev'essere pubblicato telematicamente dalla autorità procedente per raggiungere la più ampia platea di destinatari (art. 13).

Se invece è richiesta la valutazione d'impatto rafforzata, tra la pubblicazione del piano di azione e la sua diffusione al pubblico, si insinua una fase istruttoria che prevede: a) la consultazione di un collegio tecnico indipendente (i cui membri sono selezionati con criteri obiettivi dall'amministrazione procedente) chiamato a verificare la adeguatezza e la precisione del piano d'azione (art. 10); l'avvio di un dibattito pubblico per permettere ai destinatari dell'azione amministrativa di partecipare al procedimento di valutazione d'impatto (art. 11, par. 1: «*ensure that those specifically affected by the system are afforded the opportunity to participate in this process*»). Al termine del percorso appena descritto l'autorità procedente pubblica in via definitiva il piano d'azione motivato sulla base dei dati istruttori raccolti (art. 12).

Da ultimo, il documento dell'ELI si preoccupa di indicare gli strumenti di tutela rispetto alla valutazione d'impatto.

Anzitutto sottolinea che l'autorità procedente possa sempre aggiornare o ripetere la valutazione in caso di errori inattesi o di sopravvenute necessità anche di ordine istruttorio (se emerge, cioè, «*substantial negative impact*» o «*additional knowledge gained during the practical use of the system*»: art. 14, par. 1 e par. 2, lett. b); in secondo luogo suggerisce di sottoporre ogni valutazione d'impatto al controllo esterno di un'autorità amministrativa indipendente (individuata esplicitamente nell'Autorità nazionale garante dei dati personali: si veda la p. 50 del documento dell'ELI) con poteri d'inchiesta, proposta e sanzionatori (art. 15), i cui provvedimenti devono sottostare in ogni caso al vaglio giurisdizionale (art. 16, par. 3).

FILIPPO D'ANGELO

https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-issues-guidance-on-the-use-of-algorithmic-decision-making-systems-by-public-administration/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=f4a2a4a677e3dcf6e391d9f0a2a9bd6a