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. Il recepimento in Italia delle direttive (UE) 2019/770 e 2019/771 relative a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali e a determinati aspetti dei contratti di vendita di beni di consumo.

Con i D.Lgs. 4 novembre 2021, nn. 170 e 173, il legislatore italiano ha dato recepimento alle direttive UE del 20 maggio 2019, nn. 2019/771 e 2019/770, rispettivamente relative a determinati aspetti dei contratti di vendita dei beni di consumo e a talune prescrizioni concernenti i contratti di fornitura di contenuti o servizi digitali (di seguito anche solo "**dir. 771**" e "**dir. 770**").

Le due direttive si collocano all'interno della medesima strategia per il raggiungimento del mercato unico digitale. Pur differenziandosi per l'ambito di applicazione, esse condividono la finalità di «contribuire al corretto funzionamento del mercato interno garantendo nel contempo un livello elevato di protezione dei consumatori», che perseguono imponendo agli Stati membri un livello di massima armonizzazione (artt. 1 e 4 di entrambe le direttive). Ciò implica che, in fase di recepimento, ai legislatori nazionali sia precluso mantenere «disposizioni divergenti» da quelle delle direttive o introdurne di ulteriori per garantire al consumatore un livello di tutela diverso.

I profili di «digitalizzazione» del mercato unico si colgono già nei profili definitori della direttiva dedicata alla vendita di beni di consumo, che integra la nozione di «bene» fino a ricomprendervi qualsiasi bene mobile materiale incorporante o interconnesso con un contenuto digitale o un servizio digitale la cui mancanza «impedirebbe lo svolgimento delle funzioni proprie del bene» (art. 2, n. 5, lett. b, testualmente riproposto all'interno dell'art. 128, co. 2, lett. e, c. cons., come sostituito per effetto del d.lgs. 173/2021).

I criteri di conformità al contratto fissati dalla dir. 771 e la responsabilità del venditore per la loro assenza sono declinati alla luce del più esteso ambito oggettivo di applicazione della dir. 771 rispetto alla precedente direttiva CE 1999/44, espressamente abrogata. I requisiti della funzionalità, compatibilità, interoperabilità, sicurezza e durabilità richiesti affinché i beni ai quali si applicano le previsioni della dir. 771 possano superare positivamente il giudizio di conformità richiedono indubbiamente un ripensamento che muova dalla diversa natura del «bene digitale». La soddisfazione del giudizio di conformità, però, pare anche assumere contorni di durata per i beni di quest'ultima categoria, perché si impone al venditore di fornire e assicurare la corretta installazione degli aggiornamenti previsti dal contratto e necessari per mantenere la conformità nei due anni successivi alla consegna.

Nonostante l'estensione dell'applicazione della disciplina della vendita di beni di consumo ai beni con elementi digitali, la dir. 771, per l'espressa esclusione operata dall'art. 1, non si applica ai contratti di fornitura di un contenuto digitale o di un servizio digitale, regolati invece dalla direttiva «gemella», la dir. 770. La necessità di coordinamento tra la dir. 770 e la dir. 771 è evidente, ma il legislatore italiano che ha curato il recepimento di ciò non ha dimostrato particolare consapevolezza, limitandosi in buona misura a trasporre all'interno del codice del consumo le previsioni delle due direttive.

Segnatamente, l'art. 1 D.Lgs. 173/2021 introduce, dopo il capo I del titolo III della parte IV c. cons., il nuovo capo I-bis (artt. 135 octies ss. c. cons.), relativo ai contratti di fornitura di contenuto digitale e di servizi digitali, mentre l'art. 1 D.Lgs. 170/2021 sostituisce integralmente il capo I del titolo III della parte IV del codice del consumo (artt. 128 ss. c. cons.), al fine di adeguarlo alle novità introdotte dalla seconda. Entrambe le modifiche al c. cons. acquistano efficacia a decorrere dal 1° gennaio 2022, ai sensi degli artt. 2 dei decreti richiamati, con l'unica differenza che le disposizioni di cui ai nuovi artt. 128 ss. si applicheranno ai soli contratti conclusi successivamente a tale data, mentre quelle di cui al nuovo capo I bis saranno applicate a tutte le forniture di contenuto digitale o di servizi digitali che avverranno a decorrere dalla presa di efficacia delle disposizioni, a prescindere dalla data di conclusione del contratto, con esclusiva eccezione delle disposizioni di cui agli artt. 135 *quindecies* e 135 *vicies semel*, relativi al diritto di regresso del professionista e alla modifica del contenuto digitale o del servizio digitale, applicabili ai soli contratti conclusi dopo il 1 gennaio 2022.

I nuovi art. 128 – 135 *septies* c. cons. ricalcano pedissequamente la struttura e i contenuti della dir. 771, il cui ambito di applicazione oggettivo è solo parzialmente coincidente con quello della dir. 1999/44/CE, dalla stessa abrogata. La «vendita» di beni di consumo si conferma essere una disciplina applicabile in via transtipica alle relazioni b2c in fattispecie contrattuali che poco o nulla hanno a che vedere con la vendita in senso tecnico, ma che ad essa sono espressamente equiparate (così, il nuovo art. 128 c. cons., stabilisce che, ai fini

dell'applicazione del capo a cui dà apertura, alla compravendita «sono equiparati i contratti di permuta e di somministrazione nonché quelli di appalto, d'opera e tutti gli altri contratti comunque finalizzati alla fornitura di beni da fabbricare o produrre». L'ampliamento del perimetro di operatività della materia, che si riflette immediatamente sui profili definitori di cui al nuovo art. 128 c. cons. e che determina una più articolata configurazione della responsabilità del venditore (ex artt. 130 e 133 c. cons.) è sostanzialmente collegato all'allargamento dell'oggetto del contratto concluso tra professionista e consumatore, che può ora riguardare anche beni con elementi digitali.

Con riguardo a quest'ultima categoria di beni, il venditore è chiamato a rispondere di qualsiasi difetto di conformità del contenuto digitale o del servizio digitale che si verifica o si manifesta entro due anni dalla consegna, ovvero per il maggiore arco temporale per il quale il contratto concluso preveda la fornitura del contenuto digitale o del servizio digitale (art. 133, co. 2 c. cons.); deve altresì, per il medesimo lasso temporale, «tenere informato il consumatore sugli aggiornamenti disponibili, anche di sicurezza, necessari al fine di mantenere la conformità» (art. 130, co. 2 c. cons.).

È peraltro verosimile ipotizzare che la possibilità di instaurare un giudizio comparativo tra le qualità ontologiche del bene e le qualità deontologiche dello stesso anche a seguito dell'errata installazione, seppur con esclusivo riferimento ai casi previsti dal nuovo art. 131 c. cons., porterà il venditore di beni con elementi digitali ad adottare particolari cautele – almeno informative – relative alla fase di installazione.

Il diritto di regresso riconosciuto al venditore «responsabile nei confronti del consumatore a causa di un difetto di conformità imputabile ad un'azione o ad un'omissione di una persona nell'ambito dei passaggi precedenti della medesima catena contrattuale distributiva» copre, ai sensi del nuovo art. 134 c. cons., anche la circostanza in cui la mancanza di conformità derivi dall'omessa fornitura degli aggiornamenti di beni con elementi digitali.

Da un punto di vista sostanziale, il recepimento degli artt. 6, 7 e 10 dir. 771 nei nuovi artt. 129 e 133 c. cons. rappresenta la novità con maggiore impatto sistematico.

Nonostante il legislatore italiano non si sia cimentato in sforzi tesi a chiarire la natura della responsabilità del venditore, la formulazione dell'art. 10, co. 1, dir. 771, a cui fa eco l'art. 133, co. 1., c. cons., secondo la quale «il venditore è responsabile nei confronti del consumatore» dei difetti di conformità sembra ormai inequivocabilmente contraddistinguere un'obbligazione del venditore di consegnare beni conformi.

La disarticolazione dei criteri di conformità su due livelli, uno soggettivo e uno oggettivo, operata a livello interno attraverso i commi 2 e 3 del nuovo art. 129 c. cons., poi, milita nella medesima direzione: oltre a parametri soggettivi di conformità, che si riferiscono alle qualità della *res* specificamente oggetto del contratto o di trattativa, al fine di essere giudicato conforme il bene deve presentare anche caratteristiche che il legislatore europeo eleva ad elementi integrativi della conformità sulla base di un'oggettivazione della ragionevole aspettativa del consumatore rispetto alla loro presenza nel bene acquistato. Rientrano tra i parametri oggettivi di conformità l'idoneità agli scopi per i quali si impiegano normalmente beni dello stesso tipo, la corrispondenza all'eventuale campione o modello messo a disposizione dal venditore, la presenza del corredo di accessori e istruzioni e quella delle qualità ragionevolmente attesi dal consumatore sulla base della natura del bene e delle dichiarazioni pubbliche rese dai professionisti intervenuti nella commercializzazione del bene.

Il grado di oggettività assunto dall'aspettativa del consumatore provocata dalle dichiarazioni pubbliche dei professionisti emerge altresì dalla disposizione di cui all'art. 135 *quinquies* c. cons., che recepisce l'art. 17 della dir. 771 ed ha per oggetto le garanzie convenzionali. Esso infatti stabilisce, nell'inciso conclusivo del primo comma, che la garanzia convenzionale vincola secondo le condizioni indicate nella pubblicità ad essa relativa se queste sono più vantaggiose rispetto a quelle effettivamente contenute nella dichiarazione di garanzia.

La norma di chiusura, l'art. 135 *septies* c. cons., che svolge il ruolo di coordinamento con le altre «altre disposizioni» dell'ordinamento svolta sino ad ora dall'art. 135 c. cons., segna forse il più significativo punto di rottura con il passato. Allineandosi con l'obiettivo della massima armonizzazione fissato dal legislatore comunitario (*ex* art. 4 dir. 771), la norma eclissa il c.d. principio di maggior tutela del consumatore ricavabile dalla formulazione del previgente art. 135 c. cons., in forza del quale parte della dottrina riteneva che, a fronte della consegna di un bene non conforme, si configurasse un concorso alternativo di rimedi tale da lasciare al consumatore la possibilità di scegliere discrezionalmente se appellarsi alla disciplina del codice civile in presenza di un difetto di conformità rientrante altresì nella nozione di vizio, ovvero

invocare i rimedi specificamente consumeristici. La nuova norma contenuta nel primo comma dell'art. 137 *septies* c. cons. rinvia infatti alle disposizioni del codice civile, facendo espresso riferimento a quelle dedicate a «formazione, validità ed efficacia dei contratti, comprese le conseguenze della risoluzione del contratto e il diritto al risarcimento del danno», ma il medesimo articolo, al secondo comma, ha cura di escludere che per tutto quanto regolato dal capo dedicato alla vendita di beni di consumo, possano trovare applicazione norme tese a garantire al consumatore un diverso livello di tutela. Per l'effetto, al consumatore si impedisce di eludere la gerarchia rimediale rigida che, salvo specifiche eccezioni, subordina la riduzione del prezzo e la risoluzione del contratto al previo infruttuoso esperimento dei rimedi conservativi di primo grado.

L'innalzamento del livello di tutela del consumatore rimane, in realtà, possibile ai sensi dell'art. 135 *sexies* c. cons. che, nello stabilire il carattere imperativo delle disposizioni, da una parte sanziona con la nullità tutti gli accordi precedenti alla comunicazione del difetto di conformità che limitino la responsabilità del venditore, dall'altra, però, consente che l'autonomia privata dei contraenti possa in qualsiasi tempo trovare spazio nella direzione opposta, ossia nel senso di adottare, all'interno della singola contrattazione b2c, pattuizioni volte a rafforzare la posizione del consumatore.

Ne scaturisce la necessità di interrogarsi su quali siano i criteri sulla base dei quali stabilire in termini oggettivi quando le condizioni contrattuali assicurino una «maggior tutela» e siano perciò da ritenersi valide, perché il giudizio circa il livello di soddisfacimento del consumatore rispetto all'utilità prefissata con la conclusione del contratto potrebbe rispondere ad una valutazione di interessi concreti che, ove rimessa all'autonomia negoziale anche in ordine ai rimedi esperibili, difficilmente potrebbe giustificare una valutazione sul merito da parte dell'autorità giurisdizionale.

Alla gerarchia verticale tra i rimedi esperibili dal consumatore è dedicato il nuovo art. 135 *bis* c. cons., che riconosce il diritto del consumatore alla riduzione proporzionale del prezzo o alla risoluzione del contratto solo quando l'inadempimento del venditore rispetto all'obbligo di conformità acquisti connotati di gravità o irreversibilità tali da giustificare un intervento sul sinallagma (art. 135 *bis*, co. 4, c. cons.), peraltro negando (art. 135 *bis*, co. 5, c. cons.) l'accesso al rimedio perentorio in tutti i casi in cui la lieve entità del difetto di conformità escluda quell'importanza dell'inadempimento che, *ex* art. 1455 c.c., legittima la risoluzione.

Ferma restando la possibilità che il venditore rifiuti il ripristino della conformità se la riparazione o la sostituzione sono impossibili o se i costi da sopportare a tal fine non rispettano il principio di proporzionalità e impregiudicate sia la tutela risarcitoria ai sensi del codice civile, così come l'autotutela dilatoria (art. 135 *bis*, co. 6, c. cons.), la libertà del consumatore è chiaramente circoscritta alla possibilità di scelta tra la riparazione o la sostituzione del bene. Anche tale opzione è tuttavia orientata dal criterio della proporzionalità del rimedio, da valutarsi, per espressa previsione normativa, con particolare riguardo alla convenienza dell'alternativa per il consumatore, al valore che il bene avrebbe in assenza del difetto di conformità e alla sua entità.

I successivi artt. 135 *ter* e *quater* sono rispettivamente dedicati alle modalità di esercizio dei rimedi di primo e secondo grado. Rispetto ai primi, il disposto attiene sostanzialmente alle modalità di esecuzione dell'intervento manutentivo. Per i secondi, invece, va segnalata indubbiamente una definitiva presa di posizione del legislatore europeo sulla configurazione assunta dal rimedio perentorio: la risoluzione è conseguenza dell'esercizio di un diritto potestativo del consumatore, esercitato mediante una dichiarazione unilaterale diretta al venditore e «contenente la manifestazione di volontà di risolvere il contratto di vendita» e, qualora il difetto di conformità riguardi solo alcuni dei beni oggetto del contratto, può essere parziale.

Il legislatore italiano ha mantenuto fede al testo della direttiva tacendo, invece, sulle modalità con cui il consumatore può ottenere la riduzione del prezzo. Ad essa è dedicato solo il primo comma dell'art. 135 *quater*, che richiama nuovamente la proporzionalità rispetto alla diminuzione di valore conseguenza del difetto di conformità come unità di quantificazione della riduzione, ma nulla dice circa le modalità operative con cui ottenerla.

Il recepimento della direttiva «gemella» (dir. 770) ha invece portato alla creazione del capo I bis all'interno del titolo III della parte IV c. cons., composto dagli artt. 135 *octies* - 135 *vicies ter*.

Da un punto di vista strutturale, l'omozigosi tra i due plessi di nuova introduzione all'interno del codice del consumo è pressoché totale. L'introduzione di un articolato che ambisce ad estendere le tutele consumeristiche previste per il difetto di conformità, con i dovuti adattamenti, ai «contratti di fornitura di contenuto digitale o di servizi digitali conclusi tra consumatore e professionista» (ex art. 135 *octies* c. cons.) è

significativa rispetto all'avvertita necessità di interventi regolatori che tengano in considerazione la digitalizzazione delle transazioni e contribuiscano alla creazione di un mercato unico digitale in cui siano evitati approfittamenti degli squilibri di potere a danno dei consumatori ed entro il quale gli operatori dell'Unione possano agire con sufficiente certezza e prevedibilità delle conseguenze (tra gli altri, Considerando 3, 6, 8 e art. 1 dir. 770).

Da qui si spiega agevolmente la scelta del legislatore europeo di caratterizzare anche la dir. 770 come provvedimento di armonizzazione massima e quella del legislatore nazionale di riproporre una norma di coordinamento delle disposizioni del nuovo capo sovrapponibile *in toto* a quella con cui si conclude il capo dedicato alla vendita di beni di consumo: invero, anche l'art. 135 *vicies ter* c. cons. preclude di applicare altre disposizioni aventi l'effetto di garantire al consumatore un livello di tutela diverso per quanto già disciplinato dalle regole settoriali. Peraltro, anche nel caso di contratti di fornitura di contenuti o servizi digitali, il carattere imperativo delle disposizioni fa comunque salva la possibilità di pattuire condizioni contrattuali di maggior favore per il consumatore (art. 135 *vicies bis* c. cons.).

L'integrazione vicendevole tra le norme che danno recepimento alle due direttive, espressamente auspicata dal Considerando 20 della dir. 770, si coglie con il solo raffronto dell'ambito di applicazione delle due e dalle esclusioni che queste operano.

Ciò che il nuovo art. 128, co. 3, c. cons. ha espressamente cura di escludere dalla propria sfera di operatività ricade invece all'interno del perimetro dell'art. 135 *octies* c. cons., esteso a «qualsiasi contratto in cui il professionista fornisce, o si obbliga a fornire, un contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si obbliga a corrispondere un prezzo» (co. 3), inclusi i contratti con i quali (co. 4) «il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista» quando questi non sono esclusivamente funzionali all'esecuzione del contratto o trattati al solo fine di assolvere gli obblighi di legge.

L'ampliamento dell'oggetto della controprestazione del consumatore avuto riguardo al trasferimento di dati personali impone un necessario coordinamento con la disciplina ad essi relativa, ed in particolare con il Reg. (UE) 2016/679 (il "GDPR") e con i D.Lgs. 10 agosto 2018, n. 101 e 30 giugno 2003, n. 196 (il "Codice Privacy"), espressamente menzionati dall'art. 135 *novies*, co. 6, c. cons. La previsione circoscrive l'ambito di applicazione dell'intero capo sostanzialmente operando esclusioni legate a specificità settoriali e disciplinari a cui i contratti richiamati sono sottoposti (co. 2 e 3), ma ha altresì cura di stabilire che, in caso di conflitto tra norme, le disposizioni dedicate alla fornitura di contenuto digitale o di servizi digitali sono recessive rispetto a quelle contenute in altri atti dell'Unione che disciplinano uno specifico settore o oggetto (co. 5), così come rispetto a quelle del diritto dell'Unione in materia di protezione dei dati personali (co. 6).

Il ruolo sovraordinato comunque riconosciuto alla tutela dei dati personali emerge a chiare lettere dal Considerando 24 della dir. 770, che guida nell'individuare quale sia l'effettiva portata innovativa del provvedimento e, quindi, delle relative norme di recepimento. Partendo dall'osservazione della prassi, in cui «la fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico», il considerando riconosce che «la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce», ma mira ad assicurare che anche all'interno di tali modelli commerciali i consumatori non siano vittime di abusi e «abbiano diritto a rimedi contrattuali».

Più che nella legittimazione in via incidentale di un'operazione economica che coinvolge la trasmissione di dati personali a fronte della fornitura di un bene o servizio digitale, allora, la novità apportata dalla dir. 770 e dagli art. 135 *octies* ss. c. cons. sta nel riconoscere la responsabilità del professionista per la violazione dell'obbligo di conformità anche quando la relazione b2c riguardi contratti del tutto estranei allo schema della vendita perché relativi ad una «fornitura digitale», e anche qualora la corrispettività del rapporto sia data dal trasferimento di dati personali.

Salvo il caso di inadempimento totale da parte del professionista (art 135 *septiesdecies* c. cons., dedicato alla mancata fornitura), che riecheggia la previsione di cui all'art. 61 c. cons. per il caso di mancata consegna, e attribuisce al consumatore il diritto di risolvere unilateralmente il contratto ai sensi delle disposizioni successive quando il professionista «ha dichiarato, o risulta altrettanto chiaramente dalle circostanze, che non fornirà il contenuto digitale o il servizio digitale», ovvero quando sia stato convenuto o risulti che questo doveva essere fornito entro un termine essenziale, la gerarchia rimediale prevista per la mancanza di conformità e articolata su un doppio grado di rimedi (ripristinatorio – manutentivo o distruttivo) è

analoga a quella prevista dal nuovo art. 135 *bis* c. cons. Lo stesso vale per le modalità di esercizio dei rimedi di secondo ordine di cui agli artt. 135 *octiesdecies*, co. 4 – 6 e 135 *noviesdecies* c. cons.

Il modello di responsabilità del fornitore di contenuti o servizi digitali per il difetto di conformità, però, attiene ormai inevitabilmente alle modalità di esecuzione della prestazione ed è indubbio che esso consegua ad un inadempimento del professionista. Proprio in ragione dell'oggetto del contratto di fornitura di beni o servizi digitali, la valutazione di conformità si emancipa totalmente da un giudizio sulle caratteristiche effettivamente riscontrabili sul bene messo a disposizione del consumatore, e va ad incidere più ampiamente su obblighi di condotta dell'operatore economico dipendenti dalla natura del rapporto e delle prestazioni in esso dedotte. Tali obblighi, come avviene nella vendita di beni di consumo di cui al capo precedente, sono determinati in relazione a parametri soggettivi e oggettivi che ne condizionano il modo di essere conforme (art. 135 *decies* c. cons., rubricato, appunto «fornitura di contenuto digitale o servizio digitale e conformità al contratto, spec. co. 4 e 5 per i requisiti soggettivi ed oggettivi di conformità; art. 135 *undecies* c. cons., dedicato agli obblighi del professionista; art. 135 *duodecies* c. cons., relativo alla responsabilità per difetto di conformità conseguente all'errata installazione).

Anche la possibilità del professionista di modificare il contenuto digitale o il servizio digitale nei casi previsti dall'art. 135 *vicies semel* c. cons., di fatto andando ad incidere sulle modalità di esecuzione del rapporto, così come il diritto di recesso riconosciuto al consumatore ad opera del secondo comma del medesimo articolo «qualora tale modifica incida negativamente sull'utilizzo del contenuto digitale o del servizio digitale o sull'accesso allo stesso da parte del consumatore, a meno che tali conseguenze negative siano trascurabili» pare un chiaro indice in tale direzione.

Nel complesso sembra potersi dire che la tecnica legislativa prescelta e le modalità di recepimento non rivelano un'attività tesa ad assicurare un effettivo coordinamento tra le previsioni del codice del consumo, ma si limitano a testimoniare uno sforzo minimo indispensabile per conformarsi alla legislazione dell'Unione nei termini stabiliti. Rimane all'interprete il compito di ricostruire la disciplina per coglierne le potenzialità innovative e assicurarne la coerenza sistematica.

FRANCESCA BERTELLI

https://www.gazzettaufficiale.it/eli/id/2021/11/25/21G00185/sg

https://www.gazzettaufficiale.it/eli/id/2021/11/26/21G00186/sg

2. Il recepimento in Germania della direttiva (UE) 2019/770.

A partire dal gennaio 2022, i contratti di fornitura di contenuti e servizi digitali (*digitale Produkte*) saranno oggetto di una regolamentazione speciale in Germania, in attuazione della direttiva (UE) 2019/770 dell'Unione europea, di armonizzazione di alcuni aspetti del diritto contrattuale relativi alla fornitura di contenuti digitali e servizi digitali. Il Bundestag ha a tal fine approvato nel corso dell'estate una legge di modifica alla disciplina del Codice civile tedesco (25 giugno 2021, BGBl. I, p. 2123). Come noto, la summenzionata direttiva trova applicazione nei confronti di tutti i contratti in cui l'obbligo di prestazione del commerciante si riferisca ad un contenuto digitale o all'erogazione di un servizio digitale, indipendentemente dalla tipologia specifica di accordo. Siffatto approccio ha evidenziato – in Germania, così come in altri ordinamenti – il problema di giustapporre la nuova disciplina nel sistema delle regole generali del contratto. Il legislatore tedesco ha essenzialmente optato per una sua implementazione nella parte generale del BGB sull'obbligazione, dedicando una sezione apposita ai contratti relativi alla fornitura di contenuti e servizi digitali (*Verträge über digitale Produkte*, §§ 327-327u BGB). Allo stesso tempo, è stata approvata anche la legge che regola la vendita di beni con elementi digitali e altri aspetti del contratto di vendita (BGBl. I, p. 2133), che attua la direttiva (UE) 2019/771 su alcuni aspetti contrattuali della vendita di beni, anch'essa destinata ad entrare in vigore all'inizio del nuovo anno. Per la portata delle disposizioni interessate, i primi commentatori hanno paragonato la riforma sui contratti su prodotti digitali alla *Schuldrechtsmodernisierung* del 2001, riconoscendo a questi accordi negoziali natura di "*neuer Vertragstyp*". In sintesi, il nuovo corpus di disposizioni generali prevede i) una definizione del contratto su prodotto digitale; ii) l'obbligo legale di aggiornamento del prodotto digitale; iii) la disciplina della garanzia sui prodotti digitali; iv) l'adeguamento delle disposizioni specifiche sui contratti di vendita generale, quelli di vendita al consumo, di *leasing*, di donazione, di opera e di servizio. Data la portata di armonizzazione massima prevista dalla disciplina euro-unitaria, agli Stati residuano margini invero angusti di discrezionalità nel suo recepimento, perlopiù limitati alla determinazione dell'estensione del periodo di

garanzia e delle procedure di conclusione del contratto. L'accento dell'impianto definitorio del contratto su prodotto digitale si colloca, in misura evidente, sulla determinazione del corrispettivo del contratto e, segnatamente, sul pagamento con dati personali dell'utente del servizio. Con la modifica del §312 (1) BGB e del §312 (1a) BGB, il legislatore persegue principalmente l'obiettivo di ampliare l'ambito di applicazione delle disposizioni di protezione dei consumatori (§312 BGB ss.) anche a quei contratti in cui il consumatore paga per le prestazioni del fornitore "*con i suoi dati*". Se finora il § 312 BGB si limitava difatti a coprire gli accordi "*che hanno come oggetto una prestazione a titolo oneroso da parte del commerciante*", le nuove disposizioni si riferiscono più genericamente all'impegno del consumatore di "*pagare un prezzo*", che può anche consistere nel "*fornire al commerciante o nell'impegnarsi a fornirgli dati personali*" (§ 312, 1a BGB). Secondo il memorandum di accompagnamento alla legge di riforma, non assume rilievo la circostanza per cui il consumatore fornisca attivamente i dati al commerciante o se il commerciante usi o elabori in altro modo i dati già a sua disposizione per ragioni diverse. Tuttavia, il §312 (1a), frase 2 BGB esclude l'applicazione di questo apparato di disposizioni quando il professionista "*tratti i dati personali forniti dal consumatore esclusivamente al fine di adempiere ai suoi obblighi di prestazione o ai requisiti legali impostigli e non li tratta per qualsiasi altro scopo*". Pertanto, se un professionista elabora, per esempio, i dati dell'indirizzo del consumatore per inviargli i beni ordinati, o se memorizza i dati di fatturazione per scopi contabili e fiscali, questo non comporta l'applicabilità delle disposizioni relative di protezione dei consumatori. La situazione ovviamente cambia qualora il professionista elabori anche l'indirizzo o i dati di fatturazione per altri scopi, ad esempio per proporre pubblicità mirate al singolo consumatore. Nei riguardi della determinazione del prezzo – oltre alla possibilità che il corrispettivo sia costituito dal pagamento con dati personali -, il § 327(1) BGB include inoltre ogni rappresentazione digitale di un valore, quale l'erogazione di buoni, *coupon*, *tokens* elettronici, cryptovalute etc. La prestazione principale in capo al professionista è quella relativa all'obbligo di fornitura del contenuto o servizio digitale (§ 327b BGB). Salvo diversa previsione contrattuale, il consumatore può richiedere la prestazione immediatamente dopo la conclusione del contratto, ossia non appena il contenuto digitale o il mezzo appropriato per accedere o scaricare il contenuto digitale è stato messo a disposizione o reso accessibile al consumatore direttamente, ovvero tramite un dispositivo designato dal consumatore a tale scopo (§327b (3) BGB). Il codice chiarisce inoltre che "*mettere a disposizione*" significa che il consumatore viene dotato di un accesso indipendente che gli consenta di impiegare un servizio sotto il controllo di terzi, non rilevando che il servizio sia effettivamente utilizzato. Un'innovazione di particolare rilievo è quella relativa all'obbligo del fornitore del prodotto digitale di assicurare gli aggiornamenti (compresi quelli di sicurezza) necessari per mantenere la conformità contrattuale del prodotto digitale entro un dato lasso di tempo (§ 327f (1) BGB). Rispetto alla portata dell'obbligo, occorre comunque notare come il riferimento alla "*conformità contrattuale del prodotto digitale*" non copra la fornitura di aggiornamenti che determinino un miglioramento funzionale del prodotto, quali, ad esempio, il rilascio di software che rendano compatibile una smart TV con applicazioni sviluppate dopo la sua messa in commercio. Il periodo in cui debba essere assicurata la messa a disposizione di aggiornamenti varia in relazione alle caratteristiche del contratto: nel caso di un contratto per la fornitura permanente di un prodotto digitale, il periodo rilevante è quello concordato di fornitura (§ 327c(1) frase 3 n. 1 BGB); in tutti gli altri casi, il periodo rilevante è quello che il consumatore può ragionevolmente aspettarsi in base alla natura e allo scopo del prodotto digitale e tenendo conto delle circostanze e della natura del contratto. Ad ogni modo, se pur non chiarendo del tutto cosa debba intendersi per "*aspettativa ragionevole*", il memorandum di accompagnamento precisa che l'obbligo di aggiornamento non debba necessariamente limitarsi al relativo periodo di garanzia. In particolare, il legislatore tedesco ritiene che possa distinguersi tra sistema operativo e software applicativo. Così, un sistema operativo per un dispositivo che richieda l'accesso a Internet dovrebbe essere fornito di aggiornamenti per un periodo di tempo più lungo a causa della sua importanza centrale rispetto al *software* applicativo il cui uso non richieda l'utilizzo di una connessione. La disciplina sui contratti a contenuto digitale introduce una significativa deroga a quella generale sulla vendita anche in punto di rimedi in caso di difformità del prodotto. In primo luogo, il consumatore ha diritto alla rimozione dei difetti, entro un tempo ragionevole dalla comunicazione e senza notevoli inconvenienti per il consumatore (§ 327l BGB). Contrariamente al diritto generale di vendita, però, il consumatore non ha il diritto di scegliere se vuole che il prodotto digitale sia riparato o reso nuovamente disponibile, sempre che questo sia

ragionevolmente possibile. Questa decisione spetta piuttosto al professionista, vale a dire quella se voglia rimediare al difetto inviando una versione aggiornata del prodotto digitale o mettendo nuovamente a disposizione una copia priva di difetti. Quando la rimozione dei difetti sia impossibile o eccessivamente gravosa per il professionista, il consumatore ha diritto a risolvere il rapporto attraverso una corrispondente comunicazione al professionista (§ 327l (2) BGB). In linea di massima, il consumatore può risolvere il contratto solo se il prodotto digitale ha un difetto che non è irrilevante (§ 327m (2) BGB). Tuttavia, questo limite non si applica se si tratta di un contratto per la fornitura di contenuti digitali e servizi digitali in cui il consumatore fornisce o si è impegnato a fornire dati personali. Tali contratti possono difatti essere risolti dal consumatore anche nel caso di un difetto di minor rilevanza, data la maggior tutela da assicurarsi al valore del dato personale quale moneta di scambio. Qualora non intenda chiedere la risoluzione, il consumatore può comunque domandare la riduzione del prezzo (§327n (1) frase 1 BGB). In caso di risoluzione del contratto, il professionista deve rimborsare al consumatore i pagamenti effettuati per adempiere al contratto e gli è fatto divieto di far uso del contenuto che il consumatore abbia fornito o creato quando ha usato il prodotto digitale fornito dal commerciante dopo la fine del contratto (§327p (2) frase 1 BGB). Nella misura in cui tali contenuti contengono dati personali, non troveranno tuttavia applicazione le disposizioni del Titolo del BGB sui contratti a contenuto digitale, quanto quelle del GDPR (che consente, a talune condizioni, il diritto del consumatore alla cancellazione del dato personale). Infine, alcune rilevanti previsioni sono dedicate alla possibilità per il fornitore di modificare in via unilaterale le caratteristiche del prodotto digitale. La legge tedesca permette queste modifiche, alle condizioni stabilite al § 327r (1) BGB, ossia che i) il contratto preveda espressamente questa possibilità, ii) ci sia un motivo valido, iii) il consumatore non sostenga costi aggiuntivi e iv) sia informato in modo chiaro e comprensibile. Il Considerando 75 della direttiva (UE) 2019/770 cita a titolo esemplificativo, i cambiamenti necessari per adattare il prodotto digitale a un nuovo ambiente tecnico o all'aumento del numero di utenti. Inoltre, se la capacità del consumatore di accedere al prodotto digitale o l'usabilità del prodotto digitale per il consumatore è compromessa nel corso della modifica del prodotto digitale, essa può essere fatta solo se il consumatore è sufficientemente informato entro un periodo di tempo ragionevole su un supporto durevole sulle caratteristiche e il tempo della modifica così come i suoi diritti legali, quali il diritto di risolvere il rapporto (salvo che il prodotto conservi la sua utilizzabilità senza costi aggiuntivi) (§ 327r BGB).

FEDERICO PISTELLI

https://dejure.org/BGBl/2021/BGBl._I_S._2123

3. Le rilevanti modifiche al Codice Privacy introdotte dal 'Decreto Capienze' del 7 ottobre 2021 come convertito in legge con modifiche ad opera della legge 3 dicembre 2021 n. 205.

Il 7 ottobre 2021 è stato approvato dal Consiglio dei Ministri, e pubblicato in Gazzetta Ufficiale il giorno successivo, il decreto-legge n. 139/2021 ("**Decreto Capienze**") con il dichiarato obiettivo di prevedere degli allentamenti alle misure anti-Covid introdotte nei mesi precedenti. Nell'ambito di tale intervento il Governo ha inteso disciplinare anche alcuni aspetti in materia di protezione dei dati personali: l'art. 9 del Decreto Capienze, infatti, ha introdotto significative modifiche al D.Lgs. 196/2003 ("**Codice Privacy"**) volte a snellire e semplificare l'attività della Pubblica Amministrazione, ma che hanno fatto molto discutere proprio per il significativo ampliamento dei poteri della Pubblica Amministrazione in materia di protezione dei dati personali e per la corrispondente riduzione dei poteri di controllo e vigilanza dell'Autorità garante per la protezione dei dati personali ("**Garante Privacy**"). Tali modifiche sono state in gran parte confermate e, anzi, ampliate dalla legge 3 dicembre 2021, n. 205 che ha convertito con modificazioni il Decreto Capienze (la "**legge di conversione**").

Un primo intervento riguarda la semplificazione nell'utilizzo delle basi giuridiche del trattamento. Il comma 1 dell'art. 9 come previsto dalla legge di conversione modifica l'art. 2-*ter* del Codice Privacy prevedendo che la base giuridica di cui all'art. 6, para. 3, lett. b) del GDPR può essere costituita non più solamente da una norma di legge o di regolamento, ma anche da "*atti amministrativi generali*". La norma, inoltre, introduce un nuovo comma 1-*bis* del Codice Privacy ai sensi del quale il trattamento da parte di un'autorità pubblica può essere consentito anche "*se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti*". Questo significa che di fatto la Pubblica Amministrazione potrà sempre trattare dati personali ogni qual volta lo ritenga necessario per lo

svolgimento delle proprie funzioni, ponendo come fondamento di tale trattamento un mero atto amministrativo.

Altra importante novità, non presente nel Decreto Capienze e introdotta in sede di conversione, riguarda la comunicazione e la diffusione di dati personali. L'art. 2-*ter* del Codice Privacy prevedeva che la comunicazione di dati personali fra titolari di trattamenti effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri fosse consentita solo in presenza di una norma di legge (o di regolamento) e, in assenza di tale norma, era necessario effettuare una comunicazione al Garante che aveva 45 giorni di tempo per indicare le misure da adottare a garanzia degli interessati. La diffusione era invece possibile solo in presenza di una norma di legge o di regolamento. Il nuovo art. 2-*ter* prevede invece che sia la comunicazione che la diffusione saranno consentite non solo se previste da una norma di legge o di regolamento, ma anche se necessarie ai sensi del comma 1-*bis* (cioè se necessarie per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri), con l'unico vincolo di doverne dare notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

La legge di conversione è intervenuta anche sul trattamento di categorie particolari di dati personali per motivi di interesse pubblico rilevante. L'art. 2-*sexies* del Codice Privacy, modificato dalla legge 205/2021, prevede infatti che anche i trattamenti delle categorie particolari di dati personali di cui all'art. 9 GDPR potranno essere previsti, oltre che da norme di legge e di regolamento, da "*atti amministrativi generali*". Per i dati personali relativi alla salute che siano "*privi di elementi identificativi diretti*" viene introdotta dal nuovo comma 1-*bis* dell'art. 2-*sexies* una disciplina specifica che prevede la definizione delle modalità e delle finalità del trattamento con decreto del Ministro della salute previo parere del Garante.

In sede di conversione è stata confermata la scelta, particolarmente criticata, di abrogare per intero l'art. 2-*quinquesdecies* del Codice Privacy che prevedeva la possibilità di un controllo preventivo da parte del Garante sui trattamenti ad alto rischio svolti per l'esecuzione di un compito di interesse pubblico, con la facoltà per l'Autorità di imporre l'adozione di misure a tutela degli interessati. Tale modifica fa venire meno un importante strumento di tutela preventiva degli interessati di cui il Garante si è più volte avvalso per evitare che alcune misure adottate dal Governo, anche nell'ambito della lotta al Covid-19 (ad esempio con riferimento all'App IO e al *Green pass*), potessero risultare in una limitazione dei diritti e delle libertà degli individui.

In un'ottica analoga si colloca il comma 7 dell'art. 9 della legge di conversione che stabilisce un termine perentorio di 30 giorni entro cui l'Autorità potrà pronunciarsi su riforme, misure e progetti del Piano nazionale di ripresa e resilienza (PNRR). Decorso tale termine il Governo potrà andare avanti senza più la necessità di acquisire il parere.

La legge di conversione ha invece eliminato la norma del Decreto Capienze che, in tema di dati di traffico, abrogava il comma 5 dell'art. 132 del Codice Privacy che attribuisce al Garante il potere di prescrivere misure a tutela degli interessati con riferimento a trattamenti finalizzati alla prevenzione di reati e di stabilire le modalità per la distruzione delle informazioni entro due anni nel caso del traffico telefonico, ed entro un anno per il traffico telematico.

Il Decreto Capienze è poi intervenuto sul reato di diffusione illecita di immagini o video sessualmente espliciti (c.d. *revenge porn*) di cui all'art. 612-*ter* c.p. Questo intervento è stato confermato e rafforzato dalla legge di conversione che ha aggiunto al Codice Privacy l'art. 144-*bis* secondo cui "*chiunque, inclusi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso ha facoltà di segnalare il pericolo al Garante*". Nel caso di minori, la segnalazione al Garante può essere fatta anche da chi esercita la responsabilità genitoriale o la tutela. Il Garante è tenuto a provvedere entro 48 ore dalla segnalazione e può adottare provvedimenti nei confronti dei gestori delle piattaforme digitali anche indicando le misure per la conservazione a fini probatori del materiale oggetto della segnalazione.

Un ulteriore rilevante intervento, non presente del Decreto Capienze e introdotto con la legge di conversione, riguarda la c.d. moratoria per i sistemi di videosorveglianza con sistemi di riconoscimento facciale. Il comma 9 dell'art. 9 della legge di conversione prevede infatti la sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale attraverso dati biometrici, in luogo pubblico o aperto al pubblico, da parte di soggetti sia pubblici che privati, fino a che non sarà adottata una disciplina specifica, e comunque non oltre il 31 dicembre 2023. Tuttavia, la portata di tale

sospensione viene ridotta dal successivo comma 12 che ne esclude l'applicabilità ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati. In questi casi, pertanto, l'utilizzo degli impianti di videosorveglianza con sistemi di riconoscimento facciale sembra essere già consentito previo parere del Garante, parere comunque non necessario se si tratta di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali o di quelle giudiziarie del pubblico ministero.

Dall'esame delle modifiche sopra riportate si può concludere che la legge di conversione ha realizzato una profonda modifica del Codice Privacy, andando ben al di là della situazione emergenziale legata al Covid-19. In particolare, se da un lato ha ampliato i compiti del Garante con riferimento al *revenge porn*, dall'altro ne ha significativamente ridotto i poteri di controllo e vigilanza nei confronti della Pubblica Amministrazione, la quale si trova ora di fatto a poter decidere in sostanziale autonomia quali dati trattare, a chi comunicarli, e se diffonderli. Il rischio è di scalfire le tutele previste in favore degli interessati esponendoli al pericolo di lesione dei loro diritti e libertà fondamentali, nonché di far emergere l'idea che la protezione dei dati personali rappresenti un ostacolo all'attività dei soggetti pubblici e che, come tale, possa essere sacrificata in nome di altri interessi considerati prevalenti.

CHIARA RAUCCIO

https://www.gazzettaufficiale.it/eli/id/2021/10/08/21G00153/sg
https://www.gazzettaufficiale.it/eli/id/2021/12/07/21G00228/sg

4. Verso il Data Governance Act: le modifiche del Consiglio dell'Unione Europea del 24 settembre 2021 alla proposta di regolamento della Commissione, approvate dal Comitato dei rappresentanti permanenti il 1 ottobre 2021 con contestuale mandato alla Presidenza del Consiglio di avviare le negoziazioni con il Parlamento Europeo.

Come noto, nel corso dell'ultimo decennio l'ingresso nel mercato di tecnologie *disruptive*, capaci di influenzare ogni settore dell'economia e della vita quotidiana, è stato accompagnato da un (sempre maggiore) utilizzo dei dati, i quali sono divenuti – in definitiva – un essenziale fattore economico trainante.

I dati rappresentano, dunque, il fulcro delle trasformazioni tecnologiche digitali cui stiamo assistendo e l'Unione Europea – che aspira a divenire *leader* di una società basata sui dati – ha adottato una propria 'strategia', con la quale essa intende dar vita a uno 'spazio comune europeo di dati'.

Nell'ambito di tale 'strategia per i dati', il 25 novembre 2020, la Commissione Europea ha adottato una proposta di regolamento relativo alla *governance* europea dei dati ("**Atto sulla *governance* dei dati**" o "***Data Governance Act***" o "**DGA**").

Tale proposta, volta a promuovere la disponibilità dei dati utilizzabili tramite il rafforzamento della fiducia negli intermediari di dati e il potenziamento dei meccanismi di condivisione dei dati in tutta l'Unione Europea, si prefigge di affrontare quattro fondamentali questioni: *(i)* la messa a disposizione dei dati del settore pubblico per il 'riutilizzo', qualora tali dati siano oggetto di diritti di terzi; *(ii)* la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma; *(iii)* il consenso all'utilizzo di dati personali con l'aiuto di un intermediario; e *(iv)* il consenso all'utilizzo dei dati per scopi altruistici.

Alla luce di tali obiettivi, l'iniziativa della Commissione va a intersecarsi con la vigente legislazione europea in materia di dati personali, all'interno della quale, come noto, godono di enorme rilevanza il Regolamento Generale sulla Protezione dei Dati (il "**GDPR**") e la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (la "**Direttiva ePrivacy**"), nonché la direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio del 20 giugno 2019 (la così detta "***Open Data Directive***"), che il *Data Governance Act* si prefigge di affiancare per integrare la disciplina del settore pubblico. Invero, l'*Open Data Directive* – che stabilisce il quadro giuridico per il riutilizzo delle informazioni e dei dati del settore pubblico – espressamente esclude dal proprio ambito di applicazione le sorti dei dati oggetto di diritti di terzi detenuti da enti pubblici (art. 1.2 lett. c) *Open Data Directive*), la cui disciplina rientra, invece, negli scopi del DGA.

Lo scorso 24 settembre 2021, il Consiglio dell'Unione Europea ha adottato – in sede di prima lettura – alcune modifiche alla proposta della Commissione, con l'obiettivo di meglio definire la relazione tra DGA e GDPR, nonché di chiarire e meglio definire in un nuovo documento, le misure già prospettate dalla Commissione, invitando contestualmente il Comitato dei rappresentanti

permanenti del Consiglio (Coreper) ad approvare il documento in guisa di mandato per la Presidenza ad avviare negoziazioni con il Parlamento Europeo. L'approvazione del testo da parte del Coreper, avvenuta lo scorso 1 ottobre 2021, permetterà dunque alla Presidenza del Consiglio di avviare tali negoziati con il Parlamento Europeo. Sia il Consiglio che il Parlamento Europeo dovranno, poi, approvare il testo definitivo.

Procedendo a illustrare i contenuti della proposta, così come modificata dal Consiglio dell'UE, è bene principiare dal **Capo I**, il quale si occupa di definire l'oggetto e l'ambito di applicazione dell'Atto sulla *governance* dei dati.

In particolare, l'art. 1 del DGA prevede che il regolamento si occupi di stabilire, senza alterare gli obblighi e i diritti racchiusi nel GDPR: *a)* le condizioni per il 'riutilizzo' di determinate categorie di dati detenuti da enti pubblici; *b)* un quadro di notifica e vigilanza per la fornitura di servizi di intermediazione dei dati; *c)* un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici.

L'art. 2 precisa poi, *inter alia*, le definizioni di:

- 'riutilizzo', per tale intendendosi "*l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico*" (art. 2.2);
- 'servizio di intermediazione dei dati', ovverosia "*un servizio commerciale, il quale ha come obiettivo principale quello di stabilire relazioni giuridiche o commerciali dirette ai fini della condivisione dei dati, mediante mezzi tecnici, giuridici o di altro tipo, tra un numero indefinito di interessati e di titolari dei dati, da un lato, e di utenti dei dati dall'altro, in particolare per l'esercizio dei diritti degli interessati in relazione ai dati personali*"; categoria dalla quale vanno espressamente esclusi i "*servizi che ottengono dati dai titolari dei dati, li aggregano, li arricchiscono o li trasformano e concedono in licenza agli utenti l'uso dei dati risultanti, senza stabilire una relazione diretta tra i titolari e gli utenti dei dati*", i "*servizi che si concentrano sull'intermediazione di contenuti, in particolare di contenuti protetti dal diritto d'autore*", "*i servizi di piattaforme di scambio di dati utilizzati esclusivamente da un titolare dei dati per consentire l'uso dei dati in suo possesso, nonché le piattaforme sviluppate e offerte esclusivamente dai produttori di oggetti e dispositivi collegati all'Internet delle Cose, il cui obiettivo principale è garantire le funzionalità dell'oggetto o del dispositivo collegato e consentire servizi a valore aggiunto*" e gli "*organismi del settore pubblico che offrono strutture di intermediazione per la condivisione dei dati su base non commerciale*" (art. 2.2a);
- 'altruismo dei dati', che indica "*la volontaria condivisione dei dati da parte degli interessati o dei titolari dei dati senza cercare una ricompensa, per obiettivi di interesse generale definiti in conformità con il diritto nazionale, ove applicabile, come ad esempio scopi di ricerca scientifica, elaborazione di politiche o miglioramento dei servizi pubblici*" (art. 2.10).

Il **Capo II** del DGA si occupa, invece, di istituire un meccanismo idoneo a consentire il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici, subordinato al rispetto dei diritti dei terzi (fra cui, ad esempio, i diritti di proprietà intellettuale, il *trade secret* e la protezione dei dati personali). L'art. 3.3 sottolinea, in particolare, che le disposizioni del Capo in parola non danno vita ad alcun obbligo in capo agli enti pubblici di consentire il riutilizzo dei dati né esentano i medesimi enti dai loro obblighi di riservatezza. Esse sono, piuttosto, volte a porre in essere una serie di condizioni basilari idonee a consentire il riutilizzo dei dati (cfr. art. 5 – condizioni che debbono essere non discriminatorie, proporzionate e oggettivamente giustificate in relazione alle finalità del riutilizzo e alle categorie e alla natura dei dati), qualora tale facoltà venga concessa dall'ente pubblico (anche dietro pagamento di una "*tariffa*" – cfr. art. 6).

Ancora, al Capo II viene introdotta la necessità per gli Stati Membri di introdurre un "*punto di contatto unico*" a sostegno dei ricercatori e delle imprese innovative per l'identificazione dei dati idonei, nonché alcune strutture volte a sostenere gli enti pubblici con mezzi di assistenza tecnica e giudiziaria.

L'art. 8a, introdotto dal Consiglio, prevede poi che – a meno che le leggi dei singoli Stati Membri dispongano un termine inferiore – le decisioni sul riutilizzo debbono avvenire entro due mesi dalla data di ricezione della richiesta (salvo possibilità di

prorogare, in casi eccezionali, il termine per ulteriori 30 giorni). Il medesimo articolo garantisce, inoltre, a ogni persona fisica o giuridica direttamente interessata da tali decisioni un diritto di ricorso avverso le medesime, la cui effettiva applicazione sarà regolata dalla legge nazionale di ciascuno Stato Membro.

Il **Capo III** rivolge, invece, l'attenzione ai requisiti applicabili ai servizi di intermediazione dei dati. In particolare, le disposizioni in esso contenute mirano ad accrescere la fiducia nella condivisione dei dati (personali e non), come pure a ridurre i costi di transazione relativi alla condivisione dei dati tra imprese (*B2B*) e da consumatore a impresa (*C2B*), grazie alla creazione di un regime di notifica per i fornitori di servizi di intermediazione dei dati.

Invero, l'art. 9 del DGA prevede che la fornitura di servizi di intermediazione dei dati (individuati dal medesimo articolo nella "*intermediazione tra le persone giuridiche titolari dei dati e i potenziali utenti*", nella "*intermediazione tra interessati che intendono mettere a disposizione i propri dati personali e potenziali utenti dei dati*" e nei "*servizi di cooperative di dati*") sia soggetta al rispetto delle condizioni previste dall'art. 11, nonché al rispetto di una peculiare procedura di notifica disciplinata all'art. 10 del DGA.

Quest'ultima disposizione stabilisce che i fornitori di servizi di intermediazione dei dati – anche qualora siano stabiliti fuori dal territorio UE (nel qual caso, sono tenuti a nominare un legale rappresentante in uno Stato Membro) – che intendano fornire i servizi di cui all'art. 9 del DGA devono presentare una notifica all'Autorità competente designata dallo Stato Membro (e comunicata alla Commissione). Una volta presentata la notifica, che deve contenere le informazioni specificamente previste dal medesimo art. 9, i fornitori possono iniziare la loro attività, tenuto conto che l'Autorità competente dovrà tenere un registro dei fornitori di servizi di intermediazione dei dati all'interno dell'Unione. Qualora, poi, uno dei fornitori cessasse le proprie attività dovrà darne notizia all'Autorità competente, la quale provvederà a informare la Commissione.

L'art. 11 del DGA, come accennato, prevede poi una serie di condizioni da rispettare nella fornitura di servizi di intermediazione dei dati, tra le quali rilevano in particolare: *1)* il divieto di utilizzare i dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e la necessità di fornire i servizi di intermediazione dei dati mediante un'entità giuridica distinta; *2)* l'utilizzo dei dati raccolti nel corso della fornitura del servizio solo per lo sviluppo di tale servizio; *3)* l'agevolazione dello scambio dei dati mediante la conversione in formati specifici, allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale; *4)* la possibilità di offrire servizi aggiuntivi volti a facilitare lo scambio di dati quali l'archiviazione, la cura, la pseudonimizzazione e l'anonimizzazione dei dati; *5)* la previsione di una procedura di accesso al servizio che sia equa, trasparente e non discriminatoria, anche per quanto riguarda i prezzi; *6)* la previsione di procedure per prevenire pratiche fraudolente o abusive in relazione all'accesso ai dati da parte di soggetti che richiedono l'accesso tramite i suoi servizi; *7)* la garanzia di una ragionevole continuità nella fornitura dei servizi; *8)* l'adozione di misure ragionevoli volte ad assicurare l'interoperabilità con altri servizi di intermediazione dei dati; *9)* l'adozione di adeguate misure tecniche, giuridiche e organizzative volte a prevenire l'illegittimo trasferimento o accesso a dati non personali; *10)* l'informare, senza ritardo, gli interessati in caso di trasferimento, accesso o utilizzo non autorizzato di dati non personali che ha condiviso; *11)* il mantenimento di un appropriato livello di sicurezza per l'archiviazione e la trasmissione dei dati non personali; *12)* la facilitazione dell'esercizio dei diritti degli interessati; *13)* la specificazione della giurisdizione o delle giurisdizioni al di fuori dell'UE in cui si intende effettuare l'utilizzo dei dati e la indicazione agli interessati degli strumenti necessari per fornire o ritirare il loro consenso al trattamento; *14)* la conservazione di un registro delle attività di intermediazione.

Sull'osservanza di tali condizioni vigila l'Autorità competente individuata da ciascuno Stato Membro, la quale si occupa altresì del monitoraggio e della supervisione del rispetto della normativa da parte dei servizi di intermediazione dei dati qualora venga richiesto da parte di persone fisiche o giuridiche (art. 13.1). L'Autorità competente ha anche il potere di richiedere ai fornitori le informazioni necessarie per verificare la conformità ai requisiti previsti dal Capo III e, qualora ne constati l'inosservanza, informa il fornitore, consentendogli di esprimere le proprie osservazioni entro 30 giorni (art. 13.3). L'Autorità ha poi il potere di ordinare la cessazione della violazione e di imporre sanzioni pecuniarie dissuasive nei confronti dei trasgressori (art. 13.4).

Sempre con riguardo al Capo III, va infine osservato che le disposizioni ivi contenute non si applicano alle organizzazioni per l'altruismo dei dati (di cui si dirà in seguito) e alle altre entità senza scopo di lucro, nella misura in cui le loro attività consistano nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da

persone fisiche o giuridiche sulla base dell'altruismo dei dati (art. 14).

All'altruismo dei dati è dedicato il **Capo IV**, il quale persegue l'obiettivo di facilitare i singoli individui e le imprese nel mettere volontariamente a disposizione dati per il bene comune. A tal fine, il DGA – che lascia notevole spazio all'autonomia organizzativa e tecnica dei singoli Stati Membri (cfr. art. 14a) – consente ai soggetti interessati di chiedere di essere iscritti a un "*registro nazionale delle organizzazioni per l'altruismo dei dati riconosciute*" (art. 15), che sarà tenuto a cura dell'Autorità competente designata da ciascuno Stato Membro (art. 20). Le organizzazioni registrate, in possesso dei requisiti di cui all'art. 16 del DGA, saranno riconosciute in tutta l'Unione Europea, creando così la necessaria fiducia nell'altruismo dei dati e incoraggiando i singoli e le imprese a 'donare' dati a tali organizzazioni, affinché possano essere utilizzati per apportare benefici sociali più ampi. Tra i requisiti imposti alle organizzazioni per l'altruismo dei dati riconosciute emerge, in particolare, l'adesione a un codice di condotta adottato dalla Commissione in collaborazione con gli *stakeholders* (artt. 16.d e 19).

Il **Capo V** del DGA stabilisce i requisiti per il funzionamento delle Autorità competenti dei singoli Stati Membri, incaricate del monitoraggio e dell'attuazione del quadro di notifica per i fornitori di servizi di intermediazione dei dati e per gli enti che praticano l'altruismo dei dati, di cui agli articoli 12 e 20. Il Capo V contiene, inoltre, alcune disposizioni volte a disciplinare il diritto dei consociati di presentare reclami contro le decisioni di tali enti e fornitori, nonché i mezzi di ricorso giurisdizionale, in relazione alle materie che ricadono nell'ambito di applicazione del medesimo DGA.

Il **Capo VI** istituisce poi un gruppo di esperti, denominato "*Comitato Europeo per l'innovazione in materia di dati*", con l'obiettivo, fra l'altro, di consigliare e assistere la Commissione nel rafforzare l'interoperabilità dei servizi di intermediazione dei dati e garantire una prassi coerente nel trattamento delle richieste di dati detenuti da enti pubblici.

Al fine di garantire condizioni uniformi di esecuzione del DGA, il **Capo VII** prevede la possibilità che la Commissione Europea adotti atti di esecuzione relativi al DGA, assistita da un comitato ai sensi del Regolamento (UE) n. 182/2011.

Infine, il **Capo VIII** del DGA contiene una serie di disposizioni transitorie e finali volte a proteggere dall'accesso e dal trasferimento internazionale illecito i dati detenuti da enti pubblici, da servizi di intermediazione dei dati e da organizzazioni per l'altruismo dei dati.

L'applicazione delle norme racchiuse nel DGA – che non dovrà incidere sull'applicazione delle disposizioni vigenti in materia di concorrenza e, in particolare, sull'applicazione degli articoli 101 e 102 del trattato sul funzionamento dell'Unione Europea ("**TFUE**") con riguardo allo scambio di informazioni sensibili dal punto di vista della concorrenza attraverso servizi di intermediazione dei dati tra concorrenti effettivi o potenziali – è prevista a decorrere dal 18° mese successivo alla entrata in vigore del *Data Governance Act* medesimo (art. 35).

Al fine, poi, di scongiurare il rischio di obsolescenza normativa, sempre insito in simili iniziative, ai sensi dell'art. 32 del DGA, la Commissione dovrà effettuare una valutazione circa l'applicazione dell'Atto sulla governance dei dati e presentare al Parlamento Europeo, al Consiglio e al Comitato economico e sociale una relazione sulle principali conclusioni tratte, entro 48 mesi dal termine indicato al menzionato art. 35.

RICCARDO ALFONSI

https://data.consilium.europa.eu/doc/document/ST-12124-2021-INIT/en/pdf

5. La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso Top System)

Il 6 ottobre 2021 la Quinta Sezione della Corte di Giustizia dell'Unione Europea si è pronunciata sulla domanda di rinvio pregiudiziale promossa dalla *Cour d'appel de Bruxelles*, nell'ambito del procedimento *Top System SA* vs. *État belge* (C-13/20), avente ad oggetto l'interpretazione dell'articolo 5, paragrafo 1, della direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore.

La controversia vede contrapporsi, da un lato, *Top System SA*, società di diritto belga che sviluppa programmi per elaboratore e fornisce prestazioni di servizi informatici e, dall'altro, *Selor*, l'ente pubblico belga responsabile della selezione e dell'orientamento dei collaboratori della pubblica amministrazione. Su richiesta di *Selor*, *Top System* aveva sviluppato diverse specifiche applicazioni. Il 6 febbraio 2008 *Selor* e *Top System* avevano concluso un contratto avente ad oggetto l'installazione e la configurazione di un nuovo

ambiente informatico di produzione, che, però, presentava dei difetti di funzionamento. Si noti che *Selor* detiene una licenza d'uso su tutti i programmi appositamente creati da *Top System*.

Il 6 luglio 2009 la *Top System* ha proposto ricorso contro *Selor* e lo Stato belga dinanzi al *Tribunal de commerce de Bruxelles*, contestando l'illegittima attività di decompilazione effettuata da *Selor* sul programma per elaboratore e richiedendo il risarcimento dei danni per la decompilazione così effettuata.

Il 26 novembre 2009 la causa è stata rinviata dinanzi al *Tribunal de première instance de Bruxelles* che, il 19 marzo 2013, ha dichiarato la domanda così proposta come infondata.

La *Top System* ha, quindi, impugnato la sentenza di primo grado dinanzi al giudice del rinvio, la *Cour d'appel de Bruxelles*, sostenendo che la decompilazione può essere effettuata solo in forza di un'autorizzazione dell'autore, o del suo avente diritto, o ancora a fini della c.d. interoperabilità - ovvero, l'interconnessione e l'interazione funzionale tra software.

Per contro, sulla base dell'interpretazione dell'art. 6 della Legge del 30 giugno 1994, che ha recepito nell'ordinamento belga la direttiva 91/250/CEE, *Selor* riteneva di essere legittimato a procedere alla decompilazione per correggere alcuni errori di funzionamento che rendevano impossibile un uso conforme alla destinazione del *software* e ad osservare, studiare e sperimentare il funzionamento del programma allo scopo di determinare le idee alla base delle funzionalità con l'obiettivo di prevenire le future interruzioni determinate da simili errori.

Alla luce dei presenti elementi di fatto ed avendo accertato l'avvenuta decompilazione da parte di *Selor*, la Corte d'Appello Belga proponeva, quindi, due differenti questioni pregiudiziali all'attenzione della Corte di Giustizia.

In merito alla prima questione, ci si domanda se l'articolo 5, paragrafo 1, della direttiva 91/250 ("Deroghe relative alle attività riservate") debba essere interpretato nel senso che il legittimo acquirente di un programma per elaboratore ha il diritto di procedere alla decompilazione di tutto o parte di esso al fine di correggere errori che incidono sul funzionamento di tale programma, anche quando la correzione consista nel disattivare una funzione che pregiudica il buon funzionamento dell'applicazione di cui fa parte detto programma.

A tal riguardo, la Corte ricorda che la decompilazione di un software è una attività di *reverse engineering* che consiste nella ricostruzione del codice sorgente partendo da un codice oggetto di un programma esistente. Attraverso la decompilazione, di regola, si ottiene un "quasi codice sorgente", non perfettamente corrispondente al codice sorgente originale. L'attività di *reverse engineering* rappresenta il contraltare, in ambito *software*, della c.d. compilazione, attività che attiene, invece, al processo di creazione del codice oggetto sulla base delle istruzioni contenute nel codice sorgente.

Siccome la decompilazione non è testualmente ricompresa tra gli atti disciplinati dall'art. 4 lett. a) e b) della direttiva, ai quali fa riferimento l'art. 5 par. 1, la Corte, nelle sue ricostruzioni, pone l'interrogativo sulla possibilità di estendere tale disciplina anche agli atti di decompilazione. A tal riguardo, la Corte sostiene che il legittimo acquirente di un programma non solo ha il diritto di decompilazione ai fini di interoperabilità a norma dell'art. 6 della direttiva, ma ha anche il diritto di decompilazione nel caso in cui ciò sia necessario per risolvere errori che incidono sul buon funzionamento del software, come previsto dall'art. 5, par. 1.

In merito, invece, alla seconda questione (ovvero, se il legittimo acquirente di un programma per elaboratore che intenda procedere alla decompilazione al fine di correggere gli errori che incidono sul suo funzionamento debba soddisfare i requisiti previsti all'articolo 6 della direttiva), la Corte chiarisce i confini ed i presupposti dell'attività di decompilazione *ex* art. 5.

La decompilazione, infatti, deve essere necessaria per la correzione di errori e per consentire al legittimo acquirente un uso conforme alla destinazione del programma; la rettifica degli errori secondo il modello dell'art. 5 deve rispettare le specifiche previsioni contrattuali che non possono in ogni modo vietare simili atti di correzione; il legittimo acquirente non può utilizzare il risultato della decompilazione per fini diversi dalla correzione di errori di funzionamento.

Pertanto, come si legge nella sentenza, il legittimo acquirente che intenda procedere alla decompilazione al fine di correggere errori di funzionamento del software potrà agire soltanto nella misura necessaria a tale correzione e nel rispetto, se del caso, delle condizioni contrattualmente previste con il titolare del diritto d'autore su detto programma, non dovendo, però rispettare i requisiti dettati dall'art. 6 della direttiva.

La sentenza in esame non solo presenta interessanti spunti di indagine circa l'ambito applicativo della tutela autoriale dei *software* ma impone anche necessarie riflessioni in merito alle nuove possibile frontiere di tutela dei programmi per elaboratore.

ENZO MARIA INCUTTI

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62020CJ0013&from=it

6. La sentenza della *Court of Appeal* del 21 settembre sul caso Dabus: l'intelligenza artificiale può essere considerata inventore?

Con sentenza del 21 settembre 2021 (*Thaler v Comptroller General of Patents Trade Marks and Designs* [2021] EWCA Civ 1374), la *Court of Appeal* del Regno Unito ha stabilito che un sistema di intelligenza artificiale non può qualificarsi come "inventore" ai sensi degli artt. 7 e 13 della legge inglese sui brevetti del 1977 (UK *Patents Act* 1977) perché non è una persona fisica. La sentenza ha confermato le precedenti pronunce dell'I*ntellectual Property Office* inglese (UKIPO) e della *High Court*, di fronte alla quale era stata impugnata la prima decisione.

La vicenda si inserisce nell'ambito della campagna internazionale di depositi di brevetto e ricorsi ("*Artificial Inventor Project*") avviata dal Dr. Stephen Thaler a partire dal 2018, per sostenere la tesi che un sistema di intelligenza artificiale debba poter essere designato come inventore in una domanda di brevetto.

Il sistema di IA in questione, denominato "DABUS" (*Device for the Autonomous Bootstrapping of Unified Sentience*), creato dallo stesso Dr. Stephen Thaler e di proprietà della società statunitense *Imagination Engines Inc*., avrebbe creato due dispositivi brevettabili che sono stati oggetto di domande di brevetto (oltre che a UKIPO) anche presso l'Ufficio Europeo dei Brevetti (EPO), lo *United States Patent and Trademark Office* (USPTO) e gli altri uffici brevetti nazionali ai sensi del Trattato di Cooperazione in materia di brevetti.

DABUS sarebbe costituito da due distinte reti neurali in grado di cooperare fra loro, elaborando concetti originali e sondandone la portata inventiva. Le due domande di brevetto riguardano, rispettivamente, un contenitore per alimenti e un particolare dispositivo di segnalazione. La prima concerne un contenitore per alimenti caratterizzato da un profilo frattale, che permette di adattarne la forma e lo rende particolarmente resistente; la seconda riguarda un dispositivo luminoso lampeggiante specificatamente ideato per far fronte a situazioni di emergenza.

Un unico filo conduttore attraversa queste domande: DABUS è nominato o dichiarato inventore, mentre il Dr. Thaler (il richiedente) è menzionato come proprietario del brevetto richiesto. Nelle domande depositate si precisa che il Dr. Thaler ha acquisito i diritti sul brevetto come proprietario, datore di lavoro e successore di DABUS.

Tra gli obiettivi del progetto c'è quello di incentivare l'innovazione utilizzando i sistemi di IA e raggiungere chiarezza, coerenza e certezza per i richiedenti di brevetti, soprattutto per quanto riguarda la questione di chi tra il proprietario, il programmatore o l'utente dell'IA dovrebbe possedere il brevetto, riducendo la nomina impropria di persone come inventori che non si qualificano come tali.

Ad oggi, tra gli uffici dei brevetti che si sono pronunciati sulla richiesta del Dr. Thaler, solamente l'ufficio sud-africano (*South Africa's Companies and Intellectual Property Commission*) ha accolto la domanda, rilasciando in data 28 luglio 2021 il primo brevetto al mondo nel quale un sistema di IA sia designato come l'inventore, e il proprietario di tale sistema (ovvero il Dr. Thaler), sia designato come titolare del brevetto.

Le decisioni degli altri uffici brevetti che hanno respinto le domande, a causa del mancato rispetto dei requisiti formali delle rispettive legislazioni sui brevetti per non aver nominato una persona fisica come inventore, sono state successivamente impugnate dal Dr. Thaler.

Mentre la corte d'appello australiana ha riconosciuto (rinviando la decisione all'ufficio brevetti) che anche l'IA possa essere riconosciuta quale inventore, l'appello avverso le decisioni dell'UKIPO, oggetto della presente analisi e quello relativo alla decisione dell'USPTO sono stati respinti.

La pronuncia dell'ufficio brevetti sudafricano e quella della *Court of Appeal* australiana sono state citate dalla *Court of Appeal* inglese, ma non sono state prese in considerazione ai fini della decisione, dato che la Corte inglese si doveva soffermare solo sull'interpretazione della vigente normativa britannica.

La *Court of Appeal* inglese a maggioranza ha respinto l'appello (*Lord Justice* Birss, dissenziente) soffermandosi su tre aspetti fondamentali:

1) È necessario che un "inventore" sia una "persona"?
2) Il Dr. Thaler poteva richiedere dei brevetti per le invenzioni di DABUS?
3) Le domande presentate all'UKIPO dovevano essere considerate ritirate ai sensi dell'art. 13 del *Patents Act*?

In merito al primo quesito tutti i giudici hanno concordato che, ai sensi dell'art. 7 del *Patents Act* 1977, solo una persona possa essere designata come "inventore". Come già precisato nella giurisprudenza precedente (*Yeda Research and Development Company Ltd v. Rhone-Poulenc Rorer International Holdings* [2007] UKHL 43), l'art. 7 del *Patents A*ct 1977 chiarisce espressamente chi abbia diritto ad ottenere un brevetto.

L'articolo 7(2) stabilisce a chi possa essere concesso un brevetto: l'articolo 7(2)(a) si riferisce all'effettivo inventore, mentre l'articolo 7(2)(b) e l'articolo 7(2)(c) elencano le altre persone che possono avere titolo ad ottenere un brevetto in qualità di aventi causa ovvero in base a previsioni normative o contrattuali.

Dalla formulazione degli artt. 7(2) e 13 (2) nonchè delle sezioni 2(4), 8 e 13(1) secondo i giudici della *Court of Appeal* risulta chiaro che solo una persona ne abbia diritto.

La seconda questione riguardava la possibilità per l'appellante di presentare domanda ai sensi dell'articolo 7(2)(b) del *Patents Act* per ottenere un brevetto.

Il Dr. Thaler sosteneva che, al momento della realizzazione delle invenzioni da parte di DABUS, avesse diritto ad esserne proprietario in virtù della dottrina dell'accessione descritta in *Blackstone's Commentaries on the Laws of England*, Ch. 26. Tuttavia, la casistica presa in considerazione da *Blackstone* riguarda nuovi beni materiali, che sono prodotti da beni materiali esistenti (ad es. i frutti degli alberi, la progenie degli animali).

Secondo tale dottrina, il proprietario del bene materiale preesistente è il proprietario del nuovo bene materiale, ma, come rilevato da *Lord Justice* Arnold, non c'è alcun riferimento all'applicazione della regola ai beni immateriali creati da beni materiali preesistenti; pertanto, nessuna norma stabilisce che il proprietario del sistema di IA sia proprietario delle invenzioni create da quest'ultima e non ha diritto a essere titolare del brevetto. A titolo esemplificativo, *Lord Justice* Arnold richiama l'ipotesi in cui una persona A scatti una foto con la macchina fotografica digitale della persona B. In tal caso la persona A e non la persona B, proprietaria della macchina fotografica, sarà la titolare dei diritti sulla fotografia (sempre che tale opera possa essere considerata tutelata ai sensi del *Copyright, Designs and Patents Act* 1988).

Infine, in merito alla terza questione, relativa alla scelta dell'UKIPO di considerare ai sensi dell'art. 13(2), ritirate le domande perché il Dr. Thaler non aveva rispettato le prescrizioni del dettato normativo per la compilazione della domanda, *Lord Justice* Birss e *Lord Justice* Arnold hanno concordato che nel fare una dichiarazione ai sensi dell'articolo 13(2) del *Patents Act* 1977, il richiedente deve solo indicare chi ritiene essere l'inventore e una domanda di brevetto non sarà respinta per "*bona fide errors*".

Su un punto la decisione, dei tre giudici della Corte d'Appello, non stata unanime: secondo *Lord Justice* Birss si doveva ritenere che il Dr. Thaler avesse presentato una dichiarazione a UKIPO, identificando al meglio delle sue convinzioni chi fosse l'inventore e il titolo derivativo di acquisto dei diritti, e pertanto, l'ufficio brevetti non avrebbe dovuto considerare ritirata la domanda. L'IPO non è tenuto ad effettuare una revisione sostanziale dell'accuratezza di qualsiasi dichiarazione. Chiunque ritenga di aver diritto ad ottenere un brevetto su quell'invenzione potrà in una fase successiva poter rivendicare il proprio diritto.

Gli altri due giudici del collegio, *Lord Justice* Arnold e *Lady Justice* Laing, invece, hanno ritenuto che mentre un controllo sostanziale dell'accuratezza di qualsiasi presentazione di informazioni ai sensi dell'articolo 13(2) non sia necessario, ciò è molto diverso dal consentire la valutazione di una domanda chiaramente non corretta. Dato che il Dr. Thaler non ha né identificato una persona come inventore nelle informazioni fornite a UKIPO né fornito un titolo derivativo valido, anche una valutazione superficiale avrebbe consentito di valutarla irricevibile ai sensi della legge.

La pronuncia della *Court of Appeal* potrebbe essere impugnata di fronte *Supreme Court*, tuttavia, potrebbe non sortire il risultato atteso dall'appellante, considerando che, come sottolineato da *Lord Justice* Arnold, molte argomentazioni contenute nell'appello del Dr. Thaler sono state proposte per una normativa futura e non prendono in considerazione le attuali norme vigenti ("*frequently put on the basis of what the law ought to be rather than it was*").

Da considerare che il giorno dopo la sentenza della *Court of Appeal*, il governo britannico ha pubblicato la sua "*National AI Strategy*", annunciata come "un nuovo piano decennale, per rendere il Regno Unito una superpotenza globale di IA". Nell'ambito di questa iniziativa, l'UKIPO lancerà nei prossimi tre mesi una consultazione sull'utilizzo degli IPRs per proteggere l'IA, da cui potrebbe derivare una soluzione legislativa.

Negli ultimi anni è evidente l'impatto dell'IA sulla proprietà intellettuale, o per meglio dire, sui sistemi di protezione basati sulla concessione di diritti esclusivi a fronte di un atto creativo o inventivo.

Il problema si pone per le cd. "*AI Generated Works*", opere dell'ingegno per le quali, come per le

invenzioni presentate dal Dr. Thaler, l'intervento umano è insignificante o del tutto assente: è possibile (ed opportuno) qualificare tali contenuti creativi e/o inventivi come proteggibili e a chi devono essere riconosciuti i relativi diritti. *Nulla quaestio*, invece, per le cd. "*AI Assisted Works*", opere create da persone fisiche ove l'IA è usata come strumento: in tal caso sarà la persona fisica ad essere considerata quale autore/inventore e titolare dei diritti.

Attualmente la maggior parte degli ordinamenti nazionali stabiliscono che le opere dell'ingegno e le invenzioni siano tutelate solo se create da persona fisica e la titolarità dei diritti non possa essere riconosciuta in capo all'IA: pertanto, se le opere creative e/o inventive sono create da IA non saranno tutelate e cadranno in pubblico dominio.

Date le opinioni divergenti dei giudici della *Court of Appeal* inglese, nonché dei togati delle altre corti che si sono pronunciate, risulta evidente che si tratta di un'importante area del diritto che non è stata ancora oggetto di interventi legislativi ma che meriterebbe di essere disciplinata nel prossimo futuro dai *policy makers*.

FRANCESCO GROSSI

https://www.judiciary.uk/wp-content/uploads/2021/10/Thaler-v-Comptroller-judgment.pdf

7. La sentenza del Tar Lazio n. 7589 del 24 giugno 2021 su algoritmi e attività amministrativa (a proposito di procedure di mobilità nella Pubblica Amministrazione)

La vicenda decisa dalla sentenza del TAR Lazio – sede di Roma, Sez. III-bis, 24 giugno 2021, n. 7589 trae origine da una procedura di mobilità nazionale all'esito della quale il Ministero dell'università e della ricerca (MIUR) ha negato ai ricorrenti – tutti docenti di sostegno in servizio presso istituti scolastici – il trasferimento in altra sede di lavoro per mancanza di un requisito oggettivo (la permanenza quinquennale nella sede d'origine) non richiesto né applicato ad altri candidati.

Risolta la questione preliminare di giurisdizione in favore del giudice amministrativo, la causa è stata trattenuta in decisione dal collegio che ha accolto il ricorso collettivo per evidente disparità di trattamento.

Il TAR Lazio ha evidenziato che il nucleo centrale della questione risiede nel fatto che l'amministrazione centrale ha deciso di gestire tutto il procedimento di mobilità attraverso un algoritmo che ha inficiato la regolarità del concorso e leso la sfera giuridica dei candidati.

Nell'accogliere l'impugnativa, il giudice romano ha notato come sia "*mancata nella fattispecie una vera e propria attività amministrativa*" dal momento che il Ministero ha devoluto a un "*impersonale*" (e quindi privo di componente umana) sistema informatico lo svolgimento della procedura di assegnazione dei docenti alle sedi lavorative disponibili in base all'organico scolastico.

L'ingente numero di concorrenti alla procedura di mobilità non poteva rappresentare un incentivo in tal senso; né consentiva di usare in via esclusiva un meccanismo matematico privo delle capacità valutative richieste per gestire la "*tradizionale e garantistica istruttoria procedimentale*" che deve informare l'attività amministrativa.

Secondo il TAR laziale un algoritmo – quand'anche impostato per tenere conto delle singole posizioni personali, dei titoli e dei punteggi – non può fornire adeguate garanzie di partecipazione e trasparenza al privato che si confronta col pubblico potere; e finisce per soppiantare l'attività umana con quella asettica di un calcolatore che non può mai svolgere una "*attività*" in senso stretto, non essendo il "*prodotto delle azioni dell'uomo*".

Così facendo l'amministrazione ha violato l'obbligo di motivazione delle decisioni amministrative e il correlato diritto alla tutela giurisdizionale perché l'assenza di un'attività amministrativa in senso specifico non ha permesso agli interessati e poi al giudice di ricostruire il percorso logico seguito dall'amministrazione per giungere alle sue determinazioni provvedimentali.

In conclusione, il TAR ha stigmatizzato l'utilizzo improprio di "*procedure informatizzate*" che eludono le regole generali dell'attività amministrativa. Il ricorso a un algoritmo rappresenta un "*modulo organizzativo*" (più di preciso uno "*strumento procedimentale ed istruttorio*") che, in ossequio al principio di legalità amministrativa, dev'essere regolato dalla legge e deve rispondere rigorosamente alle finalità da questa indicate.

FILIPPO D'ANGELO

https://www.giustizia-amministrativa.it/dcsnprr

8. L'ordinanza del 16 settembre 2021 del Garante Privacy a proposito del sistema

software di supervisione degli studenti "Respondus" impiegato dall'Università Bocconi di Milano per le prove scritte di esame

Il 16 settembre 2021 il Garante per la protezione dei dati personali ("**Garante Privacy**" o l' "**Autorità**") ha dichiarato l'illiceità del trattamento effettuato dall'Università Commerciale "Luigi Bocconi" di Milano (di seguito, la "**Università**") a mezzo di un sistema software di supervisione (*proctoring*) impiegato dall'Università nell'ambito dell'espletamento delle prove scritte d'esame al fine di identificare gli studenti e di verificarne il corretto comportamento, con conseguente adozione *inter alia* di provvedimenti ai sensi degli artt. 2-*decies* del d.lgs. n. 196/2003 ("**Codice Privacy**") e 58, par. 2 del Regolamento UE n. 2016/679 ("**GDPR**").

In risposta all'impossibilità di sostenere gli esami in presenza dovuta all'emergenza epidemiologica da SARS-CoV 2, l'Università adottava, come modalità alternativa, lo svolgimento di prove scritte a distanza, la cui genuinità sarebbe stata garantita dall'impiego del *software "Respondus"* quale sistema di *proctoring*. Nello specifico, tale *software*, tra le altre funzionalità, inibiva anzitutto l'utilizzabilità del *browser* da parte dello studente, procedendo quindi, tramite la sua articolazione *"Respondus Monitor"*, a catturare le immagini video e lo schermo degli esaminandi e a individuarne eventuali condotte sospette, mediante registrazione video e acquisizione di istantanee a intervalli regolari. Quest'ultime, debitamente contrassegnate, venivano poi messe a disposizione dei docenti, cui erano riservate le valutazioni in merito.

Snodo centrale nel *rationale* del provvedimento è l'affermazione dell'assenza di un'idonea base giuridica per i trattamenti posti in essere mediante il menzionato sistema di supervisione. *In primis*, nonostante l'Università avesse negato, con apposita rettifica in sede di memorie difensive, l'avvenuta estrazione di campioni biometrici, l'operatività del *software "Respondus Monitor"* (raccolta, elaborazione e analisi dei video acquisiti tramite apposito algoritmo, con eventuale *flag* dei comportamenti anomali) veniva qualificata dal Garante come trattamento di dati biometrici, secondo la definizione dell'art. 4, par. 1, n. 14 del GDPR (*"i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici")* relativi all'immagine facciale degli studenti. L'Autorità, inoltre, richiamava il proprio provv. 26 luglio 2017, n. 345, nel quale si ammoniva che *"nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell'individuo (...) siano automatizzati mediante l'ausilio di appositi strumenti software o hardware"*. Com'è noto, la delicatezza di tale categoria di dati personali ne fonda l'inclusione tra i cc.dd. dati particolari, destinatari dell'elevata protezione offerta dall'art. 9 del GDPR che, a fronte di un generale divieto, ne autorizza il trattamento alle sole condizioni *ivi* previste "*ed in conformità alle misure di garanzia disposte dal Garante*". Ebbene, la base giuridica dei trattamenti veniva individuata dall'Università nel consenso del singolo studente, al quale era comunque espressamente concessa, in caso di rifiuto, la possibilità di sostenere la prova con modalità alternative da concordare col docente. Alla delineazione della base giuridica del consenso, il Garante Privacy ha opposto due obiezioni, in primo luogo affermando che tale base non può invocarsi nemmeno in astratto laddove il trattamento sia (come nel caso di specie) finalizzato al rilascio di titoli di studio aventi corso legale, posto che tale attività integra il perseguimento di una finalità di interesse pubblico sprovvista di una adeguata normazione in punto di previsione di garanzie degli interessati, ai sensi dall'art. 9, par. 2 lett. *g*) del GDPR e dell'art. 2-*sexies* del Codice Privacy; e, in secondo luogo, obiettando che in ogni caso, nella fattispecie concreta, il consenso degli studenti non era libero. Quanto a quest'ultimo aspetto, il Garante Privacy ha ritenuto che nella fattispecie concreta, era difettata una "manifestazione di volontà libera" *ex* art. 4, par. 1, n. 11) del GDPR, in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento, richiamando in proposito il Considerando n. 43 del GDPR, e motivando ulteriormente l'esistenza dello squilibrio con la possibilità che il sistema adottato dall'Università generasse negli studenti il "*timore di subire ripercussioni negative, anche indirette, da parte dei docenti come conseguenza del rifiuto*". Quanto al primo aspetto, il Garante Privacy sembra aver instaurato un rapporto di prevalenza, in favore della seconda, tra le due basi di esclusione del divieto di cui alle lettere *a*) (consenso) e *g*) (motivi di interesse pubblico normati in punto di garanzia per gli interessati) di cui al par. 2 dell'art. 9 del GDPR, nel senso di ritenere unicamente rilevante accertare la sussistenza delle condizioni per l'esclusione del divieto per motivi di interesse pubblico, ricorrendo simili motivi, ed irrilevante la base del consenso. In

particolare, il Garante Privacy ha osservato che l'elemento cardine che consente l'esercizio della libertà di insegnamento (art. 33 Cost. e art. 1 l. 30 dicembre 2010, n. 240) tanto a soggetti pubblici quanto a privati risiede nel perseguimento di finalità di interesse pubblico e che,per tale ragione, la base giuridica dei trattamenti in questione andava correttamente ricercata nell'art. 9, par. 2, lett. *g*) del GDPR, non potendo, per contro, rinvenirsi tale base nel consenso e/o nel contratto. Ai sensi della citata disposizione di cui alla lett. *g*) del par. 2 dell'art. 9 GDPR, il divieto di cui al par. 1 del medesimo articolo non opera se *"il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"*. Tale prescrizione è poi ulteriormente declinata e precisata all'art. 2-*sexies* del Codice Privacy (come modificato ad opera del d.lgs. 10 agosto 2018, n. 101), che subordina l'ammissibilità dei trattamenti di dati particolari necessari per motivi di interesse pubblico alla previsione nell'ordinamento domestico di apposite *"disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"*.

Ciò premesso, constatato il difetto, nella legislazione italiana, di una norma in grado di soddisfare le illustrate garanzie, il Garante Privacy concludeva per l'assenza di un'idonea base giuridica a fondamento dei trattamenti di dati biometrici effettuati dall'Università mediante il *software "Respondus"*, in violazione degli artt. 5, 6 e 9 del GDPR e dell'art. 2-*sexies*, comma 1, del Codice Privacy. Inoltre, le predette argomentazioni venivano riproposte nel provvedimento per sostenere l'illiceità dei trattamenti anche alla luce della qualificabilità delle operazioni poste in essere dal sistema di *proctoring* come produttive di una "profilazione" degli studenti. Infatti, nonostante la valutazione di merito circa le condotte degli studenti fosse rimessa ai docenti, l'oggetto di tale giudizio era formato, secondo i rilievi del Garante Privacy, dalle sole ipotesi previamente analizzate e contrassegnate dall'algoritmo, integrando così, ad avviso della medesima Autorità, un *"trattamento automatizzato di dati personali (...) per valutare determinati aspetti personali relativi a una persona fisica"* sussumibile nell'ampia definizione di "profilazione" di cui all'art. 4, par. 1, n. 4 del GDPR. Secondo il Garante Privacy, i pericoli che ne derivano si compendiano essenzialmente nel rischio di generare informazioni diverse e ulteriori rispetto a quelle fornite dall'interessato.

Tale ultimo aspetto, ad avviso del Garante Privacy si è concretamente verificato nel caso di specie, posto che è risultato che *"Respondus Monitor"* teneva traccia dell'attività dell'esaminando durante la seduta (disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un'applicazione all'altra o per uscire dal sistema; applicazioni in uso; posizione del viso dello studente). Da ciò l'ulteriore questione del rispetto dei principî di minimizzazione e di limitazione della conservazione di cui all'art. 5, lett. *c*) ed *e*) del GDPR. Ai sensi dell'art. 25 del GDPR, essi devono essere attuati dal titolare del trattamento *"fin dalla progettazione"* e *"per impostazione definita"*, anche in caso di impiego di prodotti o servizi realizzati da terzi. Ebbene, ad avviso dell'Autorità, con riferimento al principio di minimizzazione, i dati personali prodotti dalla profilazione sono risultati sovrabbondanti e non necessari per garantire il regolare svolgimento della prova e la sua validità. Per quanto concerne la durata di conservazione delle informazioni, anche in ossequio al principio dell'*accountability*, il Garante Privacy ha osservato che è prescritta un'esplicitazione *ex ante* in maniera certa e documentabile, essendo insufficiente tanto il mero riferimento alla facoltà per l'Università di chiedere in qualsiasi momento la cancellazione dei dati, prevista nell'accordo sul trattamento stipulato col fornitore, quanto il suo esercizio al termine delle sessioni d'esame e del procedimento di valutazione delle prove. La genericità di tali indicazioni, secondo l'Autorità, non consentiva peraltro una corretta informazione preventiva dell'interessato né una compiuta *"valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità" (art. 35, par. 7, lett. b) del Regolamento), anche con riguardo alla "limitazione della conservazione (articolo 5, paragrafo 1, lettera e))"*. Per tali ragioni, il Garante Privacy rilevava l'illiceità del trattamento per violazione degli artt. 5, par. 1, lett. *c*) ed *e*) e 25 del GDPR.

Gli illustrati profili di illiceità, come emerge dal punto precedente, si riverberano sull'obbligo di informazione preventiva di cui è gravato il titolare del trattamento ai sensi degli artt. 5, par. 1, lett. *a*), 12 e 13 del GDPR, attuativo del principio di liceità, correttezza e trasparenza. In proposito, l'Autorità ha rilevato che l'informativa fornita agli studenti dall'Università risultava gravemente incompleta, anzitutto per aver omesso di menzionare diverse

forme di trattamento operate dal sistema *"Respondus"* quali: il tracciamento delle condotte durante la seduta d'esame, le successive elaborazioni mediante profilazione (cfr. Considerando n. 60 del GDPR), la registrazione audio-video della prova, l'acquisizione di un'istantanea dell'interessato all'inizio della prova. Inoltre, come già evidenziato, l'Autorità ha ritenuto difettare una precisa indicazione delle tempistiche di conservazione dei dati acquisiti. Infine, il Garante Privacy rilevava che non veniva fatto riferimento alcuno al trasferimento dei dati personali in ordinamenti extra-UE – nel caso di specie, nell'ordinamento USA, ove ha sede la società *Respondus Inc.*, fornitore del servizio e responsabile del trattamento – e, *a fortiori*, alla base giuridica dello stesso. Peraltro, l'Autorità affermava che le carenze tratteggiate non potevano ritenersi "compensate" dal rinvio, mediante *link* ipertestuale inserito nell'informativa, a pagine *web* dell'Università deputate genericamente a illustrare i trattamenti effettuati con riguardo alla "*esperienza scolastica, accademica o professionale, al titolo della tesi, al titolo del progetto finale, alla durata degli studi e ai risultati degli esami [nonché alla] documentazione sulla valutazione del vostro lavoro"*, né tantomeno dalla rappresentazione in forma orale del funzionamento del *sowftware "Respondus"* ai soli rappresentanti degli studenti. Alla deficienza del compendio informativo fornito agli interessati, poi, si accompagnava una presentazione *"frammentaria e disorganica"*. Ciò conduceva il Garante a rilevare la non conformità dei trattamenti al principio di liceità, trasparenza e correttezza, in violazione degli artt. 5, par. 1, lett. *a*), e 13 del GDPR.

Un ulteriore profilo di illiceità concerneva (oltre che la relativa informativa, di cui si è detto *supra*) la stessa esportazione dei dati acquisiti nell'ordinamento USA (ove, come detto, è stabilita la società *Respondus Inc.*, responsabile del trattamento). Com'è noto, ai sensi dell'art. 44 del GDPR, i trasferimenti internazionali sono ammessi solo nel rispetto delle condizioni previste agli artt. 45-49 del GDPR, così articolate: le decisioni di adeguatezza assunte dalla Commissione europea (art. 45) all'esito di un giudizio olistico di equivalenza sostanziale dell'ordinamento straniero sul livello di protezione dei dati personali; la prestazione di adeguate garanzie da parte del titolare del trattamento (artt. 46 e 47), fra cui spiccano le clausole tipo adottate dalla Commissione europea, oltre alle norme vincolanti d'impresa; infine, le deroghe *ex* art. 49, accessibili solo *"in caso di trasferimenti occasionali e non ripetitivi"* (cfr. le "Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679", adottate il 25 maggio 2018 dal Comitato europeo per la protezione dei dati). In data 16 luglio 2020, la c.d. sentenza *Schrems* II della Corte di Giustizia dell'Unione Europea (causa C-311/18) dichiarava invalida la decisione di adeguatezza n. 2016/1250, che avallava il c.d. *Privacy Shield* statunitense e suggellava la sostanziale equivalenza degli ordinamenti USA e UE in punto di protezione dei dati personali [sul punto 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*]. Caduto tale canale preferenziale, l'originario accordo tra l'Università e la *Respondus Inc.*, non potendo più fondare il trasferimento sull'adesione dell'impresa al *Privacy Shield*, veniva emendato mediante ricorso, con un atto aggiuntivo *ad hoc*, alle clausole contrattuali tipo avallate dalla Commissione europea con la decisione n. 2010/87 del 5 febbraio 2010. Tuttavia, l'Autorità rilevava che il rinnovato accordo ometteva di indicare le misure tecniche e organizzative di sicurezza predisposte dall'importatore, la cui descrizione era accessibile esclusivamente a seguito di apposita richiesta inoltrata attraverso uno specifico modulo *online*. Di più. Secondo il Garante Privacy, l'Università, di fatto, non era neppure in grado di aver contezza delle misure effettivamente adottate dall'importatore nei singoli trattamenti. Ciò – rilevava l'Autorità - si poneva anzitutto in contrasto con gli artt. 4, par. 1, lett. *c*) e 5, lett. *c*) delle clausole standard ma soprattutto, in tal modo, gli interessati erano privati del tutto della facoltà di far valere nei confronti dell'esportatore gli impegni contrattualmente assunti in materia di sicurezza, in violazione dell'art. 3, par. 1 delle clausole tipo allegato alla citata decisione n. 2010/87. Tali rilievi, da ultimo, portavano il Garante Privacy a ritenere che il descritto *deficit* contenutistico che inficiava *in parte qua* l'accordo tra l'Università e la *Respondus Inc.* rivelasse l'assenza di una previa verifica dell'esportatore circa l'effettiva capacità delle misure poste dall'importatore a garanzia del rispetto degli obblighi di protezione assunti. Le suesposte argomentazioni venivano poste alla base della declaratoria di illiceità dei trasferimenti in oggetto per violazione degli artt. 44 e 46 del GDPR.

L'ultimo aspetto affrontato dal Garante Privacy riguarda la valutazione di impatto sulla protezione dei dati personali (DPIA), che il titolare del trattamento è tenuto a effettuare ove *"un tipo di trattamento, allorché preved[a] in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, [possa] presentare un rischio elevato per i diritti e*

le libertà delle persone fisiche" (art. 35 del GDPR)*"*. Secondo l'Autorità, la valutazione dell'Università si dimostrava inadeguata, succinta e non puntuale, tanto nella verifica della necessità e della proporzionalità dei trattamenti in relazione alle finalità (massimamente, sotto il profilo dell'eccessività della "profilazione") quanto nell'analisi dei rischi e nella conseguente adozione di misure appropriate.

In conclusione, l'insieme dei rilievi tratteggiati conduceva il Garante Privacy, *inter alia*, a: dichiarare l'illiceità dei trattamenti posti in essere dall'Università per violazione degli artt. 5, par. 1, lett. *a*), *c*) ed *e*), 6, 9, 13, 25, 35, 44 e 46 del GDPR, nonché 2-*sexies* del Codice Privacy; dichiarare la conseguente inutilizzabilità dei dati personali trattati, ai sensi dell'art. 2-*decies* del Codice Privacy; disporre, nell'esercizio dei poteri correttivi di cui all'art. 58, par. 2, lett. *f*) del GDPR, la limitazione del trattamento, vietando all'Università ogni ulteriore operazione di trattamento con riguardo ai dati biometrici degli studenti e ai dati sulla cui base viene effettuata la profilazione degli interessati mediante il sistema "*Respondus*", nonché vietando il trasferimento dei dati personali degli interessati negli Stati Uniti d'America in assenza di adeguate garanzie per gli stessi; ingiungere all'Università il pagamento della somma di euro 200.000,00 a titolo di sanzione amministrativa pecuniaria *ex* artt. 58, par. 2, lett. *i*) e 83, par. 5 del GDPR (e fatta salva la facoltà di pagamento dell'importo ridotto ex art. 166 co. 8 del Codice Privacy).

VALENTINO RAVAGNANI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988

9. L'apertura della prima finestra temporale sulla sandbox regolamentare per i progetti fintech di cui al Decreto del MEF n. 100 del 30 aprile 2021

Il 30 settembre 2021 la Banca d'Italia, la Consob e l'Ivass (da ora anche le "**Autorità di vigilanza**" o le "**Autorità**") hanno diffuso un comunicato stampa congiunto in cui annunciavano l'avvio della prima finestra temporale, dal 15 novembre 2021 al 15 gennaio 2022, per presentare le richieste di ammissione alla sperimentazione fintech nell'ambito della sandbox regolamentare.

Il comunicato dà seguito al Decreto del Ministero dell'economia e delle finanze n. 100 del 30 aprile 2021 (da ora anche il "**Regolamento *sandbox***") entrato in vigore il 17 luglio 2021 in attuazione della delega conferita con l'art. 36, commi 2 *bis* e ss. D. L. n. 34/2019 (c.d. "Decreto crescita") e disciplinante proprio la menzionata sperimentazione.

La *sandbox* regolamentare è un ambiente controllato dove gli operatori del settore, come definiti infra, possono sviluppare progetti innovativi in ambito bancario, finanziario e assicurativo sotto la vigilanza e con il supporto delle competenti Autorità. La *sandbox* intende incentivare l'adozione di soluzioni tecnologiche e il loro ordinato impiego nei suddetti settori. La costante sorveglianza delle Autorità, da un lato, tutela la stabilità finanziaria, gli interessi dei consumatori e dei concorrenti e il buon funzionamento del mercato. Dall'altro, consente alle medesime Autorità di monitorare l'evoluzione del mercato e gestire sin da subito eventuali nuovi rischi associati all'impiego delle soluzioni in fase di sperimentazione.

Il Regolamento *sandbox* precisa che i partecipanti a quest'ultima possono essere operatori fintech, ossia soggetti, pure non vigilati, che svolgano o intendano svolgere attività fintech anche in misura non prevalente (art. 1). Possono partecipare anche intermediari vigilati dalle competenti Autorità e con sede legale o succursale in Italia ovvero con sede legale negli Stati membri dell'UE ed operanti in Italia in regime di libera prestazione di servizi. Sono esclusi dalla partecipazione alla *sandbox* coloro i quali siano assoggettati ad una procedura concorsuale o non abbiano depositato il bilancio negli ultimi 5 anni.

La soluzione da sperimentare deve riguardare i settori bancario, finanziario o assicurativo ed essere: i) "*soggetta all'autorizzazione o all'iscrizione in un albo, elenco o registro da parte di almeno una delle autorità di vigilanza*", oppure esentata dalla suddetta iscrizione; ii) prestata "*in favore di un soggetto vigilato o regolamentato da almeno un'autorità di vigilanza … avente in Italia la propria sede legale o una succursale",* ovvero in favore di un ente con sede legale negli Stati membri dell'UE ed operante in Italia in regime di libera prestazione di servizi; iii) "*svolta da un soggetto vigilato o regolamentato da almeno un'autorità di vigilanza … avente in Italia la propria sede legale o una succursale",* ovvero da un ente con sede legale negli Stati membri dell'UE ed operante in Italia in regime di libera prestazione di servizi" (art. 5).

Per essere ammesse alla sperimentazione, è altresì necessario che l'attività: i) sia "*significativamente innovativa",* ossia avvalendosi delle nuove tecnologie fornisca prodotti o servizi prima non esistenti, oppure oggettivamente diversi da quelli già noti, nei settori bancario, finanziario o

assicurativo. È altresì innovativa la soluzione che utilizzi tecnologie già in uso in nuovi modelli di business; ii) presupponga una deroga ai provvedimenti adottati dalle Autorità di vigilanza; iii) crei valore aggiunto tanto per gli utenti quanto per il mercato; iv) sia in uno stato di sviluppo talmente avanzato da consentire la sperimentazione; v) sia economicamente sostenibile (art. 6).

È possibile stabilire un numero massimo di progetti ammissibili alla sperimentazione, che non può durare più di diciotto mesi, salvo proroghe concesse dall'Autorità di vigilanza. Coloro i quali siano interessati a partecipare, e necessitino di chiarimenti, possono avviare dei colloqui informali preliminari alla presentazione della domanda beneficiando del supporto delle Autorità (art. 8). Dopo aver presentato la richiesta di ammissione, la Banca d'Italia, l'Ivass e la Consob, singolarmente o congiuntamente a seconda dell'ambito di applicazione del progetto presentato, condurranno un'istruttoria (art. 12), comunicandone gli esiti al Comitato fintech. Quest'ultimo, ai sensi del citato Regolamento sandbox, monitora l'evoluzione del settore fintech sia a livello nazionale che sovranazionale, formula proposte normative, agevola l'interlocuzione tra gli operatori di settore e le Autorità che decidono sull'ammissione alla sperimentazione. L'ammissione è comunicata al partecipante, comporta la sua iscrizione in apposito registro tenuto dal Comitato ed è revocabile nei casi di cui all'art. 14, comma 1, lett. d) Regolamento *sandbox*.

Durante la sperimentazione ciascuna Autorità vigila sulle attività svolte e può adottare i provvedimenti di cui agli artt. 13 e 14 Regolamento *sandbox* per il proprio settore di competenza, inclusa soprattutto la deroga per diciotto mesi, salva diversa disposizione, alla regolamentazione emanata dalla stessa Autorità di vigilanza.

Per disciplinare gli incombenti nascenti dal citato Regolamento *sandbox* la Banca d'Italia, la Consob e l'IVASS hanno emanato ciascuna un proprio regolamento (da ora anche i "**Regolamenti**") disciplinante l'emanazione, per quanto di competenza, dei provvedimenti di ammissione alla sandbox. Si tratta rispettivamente: del Regolamento di Banca d'Italia del 3 novembre 2021, pubblicato sulla G.U. del 10 novembre 2021; della delibera Consob n. 22054 del 27 ottobre 2021, pubblicata sulla G.U. del 5 novembre 2021 e del regolamento IVASS n. 49 del 3 novembre 2021 pubblicato sulla G.U. del 13 novembre 2021. I Regolamenti sono pressoché equivalenti tra di loro, differenziandosi solo per le Autorità di cui disciplinano l'azione, consentendo una trattazione congiunta e non introducono significative novità rispetto al Regolamento *sandbox*.

Per quanto da essi non espressamente disciplinato si applicano i regolamenti generali sui procedimenti amministrativi delle rispettive Autorità (art. 1). Tutti i Regolamenti individuano le unità organizzative responsabili del procedimento di ammissione alla sperimentazione nel loro Allegato I (art. 3) e i requisiti che deve avere la relativa domanda (art. 5). Come già stabilito nel Regolamento *sandbox*, le Autorità potranno chiedere chiarimenti e integrazioni agli interessati sulle domande da loro presentate che, in caso di inottemperanza alla richiesta nel termine stabilito (art. 6), sono rigettate. Anche l'istruttoria e la conclusione del procedimento di ammissione (artt. 7 - 10) sono disciplinati similmente al Regolamento sandbox. A partire da tali fasi, inoltre, ciascuna Autorità di vigilanza può chiedere la formulazione di un parere al Comitato fintech o ad un'altra di esse per i settori di rispettiva competenza. Infine, tanto la proroga e la conclusione del periodo di sperimentazione (artt. 13 e 16), quanto la revoca dell'ammissione a quest'ultima (artt. 14 e 15), su istanza di parte o d'ufficio, sono disciplinati analogamente al Regolamento *sandbox*, seppur con maggior dettaglio.

EMANUELE STABILE

https://www.bancaditalia.it/focus/sandbox/index.html

10. Il rapporto del 13 ottobre 2021 dei Ministeri dell'Economia e delle Banche Centrali dei Paesi G7 "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)"

Il 13 ottobre 2021 i Ministeri dell'Economia e le Banche Centrali dei Paesi G7 hanno pubblicato il rapporto "*Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)*" ("**il Rapporto**"). Il Rapporto si propone di delineare dei principi generali da considerare nella ideazione e configurazione di una *Retail Central Bank Digital Currency* ("**CBDC *retail***").

Una CBDC *retail* costituirebbe una forma di moneta di banca centrale digitale direttamente accessibile al pubblico e destinata a un uso diffuso. Fungerebbe, quindi, da complemento al contante. Il Rapporto non esclude comunque iniziative volte allo sviluppo di CBDC *wholesale*, vale a dire una CBDC il cui uso sarebbe limitato ai pagamenti

all'ingrosso e il cui accesso sarebbe ristretto alle sole istituzioni finanziarie regolamentate.

Il Rapporto è il risultato di una più ampia fase di indagine avviata nel giugno 2021 dai Ministeri dell'Economia e Banche Centrali G7 sulle implicazioni dello sviluppo di una CBDC *retail*. Si tratta di principîche dovrebbero fungere da guida. Il G7 riconosce, infatti, che la decisione sull'emissione e configurazione di una CBDC è competenza delle autorità nazionali. Tuttavia, il Rapporto evidenzia anche come dei principî comuni potrebbero affermare alcuni valori condivisi rilevanti, quali trasparenza, aderenza al quadro normativo e buon governo economico.

Il Rapporto delinea, in particolare, tredici principî a cui la configurazione e lo sviluppo di una CBDC *retail* dovrebbero ispirarsi, tenendo conto sia delle *foundational issues* che una CBDC dovrebbe fronteggiare (es. mantenimento di un adeguato livello di competizione nell'ambito dei pagamenti digitali), sia delle *opportunities* che ne potrebbero scaturire. Tra le *opportunities*, il Rapporto segnala come le CBDCs potrebbero promuovere l'innovazione digitale, stimolare una maggiore inclusione finanziaria e favorire la conduzione di transazioni *cross-border*. Focus del rapporto sono anche le *dependencies* che potrebbero sussistere tra i diversi principî. Il G7 riconosce come un approccio *one size fits all* non sia perseguibile, sicché la configurazione e sviluppo di una CBDC dovrà aversi in ciascun caso rispetto agli specifici obiettivi che si intendono conseguire, tenendo sempre però conto dei valori e dei principî generali.

Una CBDC dovrebbe, *in primis*, preservare la stabilità monetaria e finanziaria, consentendo alle banche centrali di adempiere al proprio mandato. In particolare, le CBDCs *retail* potrebbero rafforzare il ruolo della moneta di banca centrale e assicurare la fiducia del pubblico. Al contempo, però, le CBDCs potrebbero anche comportare alcuni rischi per il sistema finanziario e, in particolare, bancario, quali, fra tutti, il rischio di sostituzione dei depositi.

Una CBDC dovrebbe, poi, proteggere la *privacy* degli utilizzatori, garantendo trasparenza circa il trattamento e l'uso dei dati. Al contempo, una CBDC e il relativo ecosistema dovrebbero anche assicurare la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo. Nel Rapporto si suggeriscono diversi modelli volti a individuare una soluzione di equilibrio, quali, ad esempio, CBDC *account* pseudo anonimi basati su tecnologie DLT.

Una CBDC e il relativo ecosistema dovrebbero essere strutturati in modo tale da minimizzare i rischi operativi e informatici, nonché da garantire efficienza energetica. Si riconosce, però, come *standard* stringenti di resilienza operativa e sicurezza potrebbero impattare sulla *performance* e la funzionalità dell'ecosistema. Un giusto equilibrio dovrà essere, quindi, individuato.

Particolare attenzione, poi, è posta ai rischi che una CBDC potrebbe avere sulla competizione nell'ambito dei pagamenti digitali. Una CBDC dovrebbe coesistere con i mezzi di pagamento esistenti, promuovendo competizione e diversità. Al riguardo, si evidenzia come sia necessario assicurare interoperabilità tra le diverse soluzioni di pagamento. Non solo, nello *statement* congiunto del G7 viene rimarcato anche come le CBDCs dovrebbero coesistere con le nuove forme private di moneta digitale- quali in particolare, gli *stablecoin*- fintantoché tali forme siano coerenti con gli obiettivi di *policy* delineati. Ne vengono, difatti, evidenziate le differenze, essendo gli *stablecoin* passività di soggetti privati che ambiscono a mantenere un valore stabile, senza però che ve ne sia certezza. Considerati i rischi significativi, il G7 rimarca come sia necessario assicurare *standard* comuni di regolamentazione da delineare secondo il principio *same activity, same risk, same regulation.*

Altrettanta rilevanza è attribuita all'uso delle CBDCs in ambito *cross-border* e, in particolare, ai rischi che ne potrebbero derivare per la stabilità monetaria e finanziaria internazionale. Secondo il Rapporto, da tenere in considerazione è il rischio per cui l'uso di una CBDC sia così significativo negli altri Paesi da determinare una sostituzione della valuta. Rischi del genere dovrebbero essere, però, soppesati dai benefici che una dimensione internazionale di una CBDC potrebbe apportare nella conduzione delle transazioni *cross-border*. Al riguardo, si sottolinea come forme di integrazione e cooperazione siano necessarie, anche con riferimento a iniziative di sviluppo internazionale.

Infine, una CBDC dovrebbe essere delineata in modo tale da incrementare l'inclusione finanziaria e non impedire, ma, anzi, ampliare l'accesso ai servizi di pagamento, anche con riferimento a un possibile impiego delle CBDC nei pagamenti da e verso il settore pubblico.

ALICE FILIPPETTA

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025234/FINAL_G7_Statement_on_Digital_Payments_13.10.21.pdf

11. Le classi di rischio dei 'Software As Medical Device' (SAMDs) alla data di piena applicazione del Regolamento 2017/745 UE sui dispositivi medicali

Il **Regolamento (UE) 2017/745** sui dispositivi medici (*Medical Device Regulation*, di seguito "**MDR**") – entrato in vigore con data di piena applicazione il 26 maggio 2021 – è incentrato sul *risk approach* e sull'implementazione del sistema di gestione del rischio, del sistema di monitoraggio post-vendita e del sistema di vigilanza.

L'attenzione è infatti focalizzata sulla sicurezza e l'efficacia dei dispositivi. Viene stabilita in capo ai produttori una responsabilità per il controllo sulla produzione e sulla commercializzazione dei dispositivi. Rispetto all'impianto normativo previgente, alcune tra le principali novità possono essere così sintetizzate.

Il MDR amplia l'ambito di applicazione della nozione prevista dalla Direttiva 93/42/CEE, per cui il numero dei *software* considerabili *medical device* è sensibilmente aumentato e ai sensi dell'art. 22 i *device* sono suddivisi in 4 classi di rischio: I, IIA, IIB, III in relazione alla destinazione d'uso e ai rischi che ne derivano. Questa classificazione è effettuata dal fabbricante secondo i criteri dell'Allegato VIII, ma mentre per i dispositivi di classe I è sufficiente una valutazione della conformità e l'apposizione del marchio CE, per i dispositivi appartenenti alle altre classi occorre un controllo più rigoroso da parte dell'Organismo Notificato come definito e disciplinato dal MDR. Infatti, qualora il dispositivo presenti un rischio alto o medio, la valutazione della conformità coinvolge anche esperti indipendenti nominati dalla Commissione e dagli Stati Membri che forniranno un parere scientifico.

Rispetto ai *software* medicali occorre poi operare una differenziazione, che prescinde dalla connessione con un dispositivo e dall'ubicazione del *software*. Nell'ipotesi in cui i *software* vengano utilizzati nel contesto sanitario, ma perseguano esclusivamente finalità generali, essi non sono considerati come dispositivi medici. Qualora, invece, tali *software* forniscano informazioni che possono essere impiegate per assumere decisioni a fini diagnostici o terapeutici ovvero qualora modifichino i dati ricevuti per fornire informazioni mediche nuove e diverse, essi vengono considerati *medical device*; si parla a tal proposito di *Software As Medical Device* (SAMD). Essi sono considerati a medio o ad alto rischio.

In particolare, mentre i *software* medicali realizzati secondo le regole di classificazione della Direttiva 93/42/CEE erano per la maggior parte in classe I (quindi non sottoposti all'obbligo di controllo dell'Organismo Notificato), ai sensi del MDR gli stessi *software* "passano" in larga misura nelle classi IIA e IIB, per le quali è necessario il controllo da parte dell'Organismo Notificato.

Tuttavia, per consentire agli Organismi Notificati *ex* MDR di prepararsi in maniera adeguata ad effettuare le necessarie valutazioni, è stata introdotta una deroga che consente, a certe condizioni, la permanenza dei dispositivi in classe I fino al 26 maggio 2024.

Tanto è stato previsto dal **Regolamento (UE) 2020/561** del Parlamento europeo e del Consiglio del 23 aprile 2020 che è intervenuto a modificare il MDR per quanto riguarda le date di applicazione di alcune delle sue disposizioni. Più precisamente, per quanto riguarda la classificazione in commento, il Regolamento (UE) 2020/561 ha sostituito il primo comma del paragrafo 3 dell'art. 120 del MDR con la seguente disposizione: "*In deroga all'articolo 5 del presente regolamento, un dispositivo di classe I ai sensi della direttiva 93/42/CEE, per il quale è stata redatta una dichiarazione di conformità prima del 26 maggio 2021 e per il quale la procedura di valutazione della conformità ai sensi del presente regolamento richiede il coinvolgimento di un organismo notificato, o un dispositivo con un certificato rilasciato ai sensi della direttiva 90/385/CE o della direttiva 93/42/CEE e valido in virtù del paragrafo 2 del presente articolo, può essere immesso sul mercato o messo in servizio fino al 26 maggio 2024, a condizione che a decorrere dal 26 maggio 2021 continui a essere conforme a una di tali direttive, e a condizione che non vi siano cambiamenti significativi nella progettazione e nella destinazione d'uso. Tuttavia, le prescrizioni del presente regolamento in materia di sorveglianza post-commercializzazione, sorveglianza del mercato, vigilanza, registrazione di operatori economici e dispositivi si applicano e sostituiscono le corrispondenti prescrizioni di cui a dette direttive.*".

Tale disposizione propone la questione di cosa debba intendersi con "*cambiamenti significativi nella progettazione e nella destinazione d'uso*", in costanza dei quali la medesima disposizione prevede che l'agevolazione cessi di operare.

Anche la commercializzazione del prodotto assume una rinnovata rilevanza, essendo sancito un obbligo di controllo nella fase successiva alla commercializzazione esteso a tutti i soggetti della filiera produttiva: fabbricante, importatore, distributore. Questa nuova ottica riguarderà anche le

strutture sanitarie che realizzano autonomamente i propri *medical device*, in quanto, sebbene tali prodotti non siano soggetti alla commercializzazione e non richiedano quindi l'applicazione del marchio CE, sono in ogni caso sottoposti alle regole previste dal MDR; pertanto, anche le strutture sanitarie sono considerate fabbricanti.

Un aspetto particolarmente attuale – vista la pandemia in corso – concerne i *software* che erogano servizi di telemedicina, in quanto possono essere considerati dispositivi medici, specialmente quando prevedono l'elaborazione di dati personali; in questo caso, si pone anche un problema di coordinamento con i principî sanciti dal GDPR.

L'impianto del MDR comporta una serie di adempimenti obbligatori per le imprese, le quali dovranno valutare: il rispetto dei requisiti; l'eventuale cambio di classe di rischio da parte del *device*; la valutazione clinica del dispositivo. Si tratta di attività cruciali, che comportano evidenti costi di *compliance*. Il settore Medtech si caratterizza così per una vera e propria catena di soggetti coinvolti: il produttore del *device*, il programmatore dell'algoritmo, il *trainer*, l'ente sanitario che lo impiega, ma anche, come visto, i soggetti coinvolti nella commercializzazione; si pongono dunque notevoli problemi in tema di responsabilità, sui quali viene da più parti auspicato un apposito intervento del Legislatore.

SUSANNA SANDULLI

https://www.salute.gov.it/portale/news/p3_2_1_1_1.jsp?lingua=italiano&menu=notizie&p=dalministero&id=5499

12. La legge dello Stato del Wyoming sulle Decentralized Assets Organizations (DAOs) del 21 aprile 2021

Lo Stato del Wyoming (USA) ha promulgato, il 21 aprile 2021, la legge nota come *Wyoming Decentralized Autonomous Organization Supplement* ("**WDAOS**") entrata in vigore il 1° luglio 2021.

La WDAOS ha introdotto una disciplina delle *Decentralized Authonomous Organizations* ("**DAO**") che, nell'attuale panorama legislativo globale, costituisce il primo intervento legislativo volto a disciplinare tale fenomeno. La WDAOS non si è spinta sino a regolare in modo dettagliato le DAO e i rapporti giuridici che da essa possono originarsi. La WDAOS ha, in effetti, adottato un'altra tecnica e ha ricondotto le DAO alla preesistente legislazione societaria, seppure con interessanti peculiarità che - anche in prospettiva sistematica - potranno costituire il fondamento di successive riflessioni.

Prima di illustrare i punti essenziali della WDAOS, si riassumono qui di seguito gli elementi identificativi comunemente associati alle DAO.

La DAO, nella sua essenza fenomenica, è una comunità digitale organizzata e composta da più soggetti.

Dopo la costituzione, la DAO viene promossa dai suoi fondatori: il primo passo successivo alla costituzione consiste, di norma, nel collocamento presso il pubblico dei *token* basati su *blockchain*. Può anche accadere che una DAO sia costituita senza alcun collocamento dei *token* e che i fondatori siano, da subito, gli stessi acquirenti di tutti i *token* emessi.

Tali *token* incorporano normalmente sia il diritto di esser riconosciuti come membri della DAO, sia gli ulteriori diritti - partecipativi e di *governance* - che di volta in volta possono venire in rilievo nel momento di proporre o adottare le deliberazioni che riguardano la DAO e il suo patrimonio.

Di solito, i fondi che costituiscono la dotazione patrimoniale iniziale della DAO sono rappresentati da criptovalute; tale dotazione patrimoniale può variare, nel corso del tempo, in conseguenza di acquisti effettuati dalla DAO con il proprio patrimonio o per effetto di successivi incrementi patrimoniali tramite emissione di nuovi *token* o apporti di altra natura.

La DAO si basa su *smart contract* e su tecnologia *blockchain* e funziona tramite algoritmi decisori, dai contenuti più o meno complessi, che consentono di evitare - in tutto o in parte - l'intervento umano in fase gestoria ed esecutiva.

La DAO è uno strumento che può essere impiegato per un ampio spettro di finalità: attività di investimento; finalità filantropiche; acquisto e rivendita di opere d'arte digitali (come gli NFT); sottoscrizione in comune di abbonamenti a *software* etc.

Le regole di governance della DAO sono cristallizzate ed eseguite tramite la *blockchain*, assicurando in tal modo la immodificabilità delle regole di funzionamento; a differenza delle forme tradizionali di associazione tra più soggetti, una DAO opera su un ecosistema digitale che - almeno in parte può funzionare in assenza di un organo a cui sarebbe altrimenti delegata l'amministrazione dell'ente e del suo patrimonio.

Ne discende che la DAO è:

i. Decentralizzata: perché non è amministrata né gestita da un organo societario/aziendale centrale (ad es. un consiglio di amministrazione, un asset manager, un comitato direttivo etc.) e perché si basa sulla *blockchain*. Le decisioni aventi ad oggetto atti e negozi giuridici che interessano il patrimonio della DAO stessa sono condivise e deliberate dall'intera community di titolari dei token, sulla base di proposte votate senza la presenza di un'autorità centrale.

ii. Autonoma: perché può eseguire operazioni di rilevanza giuridica (ad es. acquisti, vendite, investimenti etc.) in autonomia e tramite l'esecuzione di algoritmi decisori e *smart contract*, quindi anche in assenza di interventi esterni o di human governance;

iii. Organizzata: perché configura un'organizzazione plurisoggettiva composta dai titolari dei token e che risponde a proprie regole, finalità e obiettivi che sono codificati negli *smart contract* ed eseguite tramite *blockchain*.

Tanto riassunto sul fenomeno socio economico, i punti salienti della disciplina della WDAOS sono i seguenti.

Innanzitutto, la WDAOS ha definito la DAO come una Limited Liability Company ("**LLC**") i cui articoli dello statuto devono contenere una dichiarazione (*statement*) in base alla quale viene reso noto al pubblico che la società è una DAO (§ 17-31-104, a). In sostanza, la legge del Wyoming non è intervenuta per definire e regolare a tutto tondo il fenomeno delle DAO, ma si è limitata a prevedere che una DAO può adottare il tipo societario previsto per le LLC, seppure con certe caratteristiche proprie che, di fatto, pongono le DAO e le LLC in un rapporto di *species* a *genus*.

Dato che, ai sensi della WDAOS, le DAO sono innanzi tutto delle LLC, la legge introduce alcune alternative statutarie tipiche per le DAO: lo statuto della DAO/LLC può prevedere, alternativamente, che la DAO sia una LLC gestita dai membri dell'organizzazione (*member managed DAO)*, oppure che la gestione sia affidata a un algoritmo (*algorithmically managed DAO*). Se lo statuto non contenesse alcuna indicazione specifica circa la forma di amministrazione, si presume che la DAO/LLC sia una *member managed DAO* (§ 17-31-104, e).

La WDAOS non contiene una definizione di *algorithmically managed DAO*. Pur in assenza di tale definizione di amministrazione algoritmica (che sarebbe stata certamente utile in prospettiva sistematica e comparativa), una LCC/DAO può essere costituita e registrata in base alle leggi del Wyoming solo a condizione che lo *smart contract* su cui si basa il sistema di amministrazione algoritmica consenta l'aggiornamento e la modifica (§ 17-31-104, d). Questa prescrizione lascia intendere che, anche laddove l'amministrazione di una DAO/LLC sia affidata a sistemi algoritmici, potrebbe non esser esclusa la responsabilità "umana" (ad es. in capo ai fondatori) per *culpa in vigilando*, ad esempio in caso di omesso aggiornamento dell'algoritmo decisorio.

La WDAOS precisa ulteriormente che la gestione di una DAO /LLC spetta ai suoi membri in caso di *member managed DAO;* invece, in caso di *algorithmically managed DAO*, in mancanza di diverse prescrizioni statutarie, la gestione spetta direttamente allo *smart contract* che implementa l'algoritmo (§ 17-31-109). Si introduce, in questo modo, la figura dello *smart contract* amministratore di società (con tutte le conseguenti difficoltà e incertezze, sul piano sistematico, che potrebbero conseguire da tale sovrapposizione tra *smart contract* e organo preposto alla gestione della società).

Altre prescrizioni degne di nota contenute nella WDAOS sono le seguenti:

i. una DAO/LLC deve avere un domiciliatario preposto alla ricezione e notifica di atti giudiziari nello Stato del Wyoming (§ 17-31-104, d);

ii. la denominazione della LLC deve includere uno dei seguenti termini "DAO", "LAO" (acronimo per *Limited Liability Autonomous Organization* ma sostanzialmente sinonimo di DAO) o "DAO LLC" (§ 17-31-104, e).

iii. lo statuto della DAO/LLC, oltre a dover dichiarare (v. supra) che la LLC è una DAO, deve contenere il seguente disclaimer (§ 17-31-104, c): *"I diritti dei membri di un'organizzazione autonoma decentralizzata possono differire sostanzialmente dai diritti dei membri di altre LLC. Il Wyoming Decentralized Autonomous Organization Supplement, gli smart contract su cui si fonda la DAO, gli articoli dello statuto […] possono definire, ridurre o eliminare i doveri delle parti e possono limitare il trasferimento della proprietà dei titoli, il recesso o l'uscita dalla DAO, nonché la restituzione dei conferimenti e lo scioglimento dell'organizzazione autonoma decentrata".*

iv. per quanto concerne la costituzione della DAO/LLC, è previsto che qualsiasi persona possa costituire una DAO e, inoltre, che la

DAO può avere uno o più soci al momento della costituzione. Il soggetto che costituisce la DAO non deve necessariamente esser socio stessa, con il che si riconosce la figura del *founder* esterno all'organizzazione (§ 17-31-105, a).

v. lo statuto della DAO/LLC deve contenere, tra le altre cose, clausole che regolino:
   a) i rapporti tra i soci e tra questi e la DAO/LLC;
   b) i diritti e gli obblighi dei partecipanti alla DAO/LLC;
   c) l'oggetto sociale della DAO/LLC e le modalità di perseguimento del medesimo;
   d) il diritto di voto e le modalità per il suo esercizio;
   e) il trasferimento dei diritti di partecipazione nella DAO/LLC;
   f) il recesso dalla DAO/LLC;
   g) i criteri di liquidazione e ripartizione tra i soci del patrimonio della DAO/LLC in caso di scioglimento;
   h) le modifiche allo statuto;
   i) le procedure per la modifica, l'aggiornamento, la modifica o la modifica degli *smart contract*.

vi. la DAO/LLC è soggetta a scioglimento e liquidazione automatica se, nel corso di un anno, non approva alcuna proposta sottoposta a votazione dai membri (§ 17-31-114, a, iv).

La WDAOS, infine, sembra attribuire massima importanza gerarchica al principio della libertà contrattuale a scapito dei principi generali societari: in base alla WDAOS, infatti, i soci di una DAO/LLC devono osservare, nei rapporti interni tra soci e con la DAO/LLC, soltanto i principi generali di buona fede e correttezza contrattuali, mentre nella DAO/LLC non trovano applicazione i *fiduciary duties* tipici delle normali LLC (§ 17-31-110).

BENEDETTO COLOSIMO

https://www.wyoleg.gov/Legislation/2021/SF0038

13. La prima legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (la 'PIPL')

Il 20 agosto 2021, dopo la discussione di due bozze, di cui la prima risalente a ottobre 2020 (su cui v. notizia n. 4 sul numero 4/2020 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf) e la seconda ad aprile 2021, l'Assemblea Nazionale Popolare della Repubblica popolare cinese ha approvato la 'Legge sulla protezione delle informazioni personali della Repubblica popolare cinese' (中华人民共和国个人信息保护法, *geren xinxi baohu fa*: di seguito "**PIPL**" dal suo acronimo già affermato in ambito internazionale).

La PIPL è la prima legge cinese interamente ed esclusivamente dedicata alla tutela delle informazioni personali e costituirà, assieme alla Legge sulla sicurezza cibernetica (2017) e alla Legge sulla sicurezza dei dati (2021), il sistema normativo cinese in materia di ICT.

Dopo aver chiarito in premessa il suo scopo, la PIPL circoscrive il suo ambito di applicazione a tutte quelle attività di trattamento delle informazioni personali compiute da organizzazioni e individui nell'esercizio della propria attività d'impresa.

La PIPL disciplina non solo il trattamento delle informazioni personali all'interno della Repubblica Popolare ma anche quelli al di fuori del territorio cinese, in determinati casi (quando il trattamento è necessario per la fornitura di prodotti o servizi a persone fisiche che si trovano all'interno del territorio cinese; quando è necessario per la valutazione o l'analisi del comportamento delle persone fisiche all'interno del territorio cinese; negli altri casi previsti dalla legge o dai regolamenti amministrativi).

Le informazioni personali sono definite, analogamente alla normativa europea in materia, come quelle 'informazioni relative a persone fisiche identificate o identificabili', ad eccezione delle informazioni rese in forma anonima.

La nuova legge pone obblighi in capo ai 'gestori delle informazioni personali' (figura analoga al 'titolare del trattamento' in ambito europeo), definiti come 'le organizzazioni o gli individui che determinano in mondo indipendente lo scopo e il metodo del trattamento'.

Tra i principi fondamentali posti dalla legge si evidenziano: il principio di liceità, di necessità e di buona fede del trattamento, il quale non deve essere mai fuorviante, fraudolento, o coercitivo, e che deve essere sempre limitato alle informazioni strettamente necessarie per lo scopo preposto; lo scopo, a sua volta, deve essere chiaramente individuato e ragionevole (vale a dire che il trattamento delle informazioni deve essere direttamente correlato a uno scopo legittimo e la raccolta di tali informazioni deve limitarsi alle sole informazioni la cui acquisizione è necessaria al

perseguimento di tale scopo); la trasparenza è richiesta in termini di regole, finalità, metodo e ambito del trattamento; l'accuratezza, secondo cui la raccolta e la conservazione delle informazioni deve essere sempre accurata, completa e aggiornata; infine, la sicurezza, per cui i gestori di informazioni personali devono garantire e adottare tutte le misure necessarie per salvaguardare la sicurezza di tutte le informazioni personali elaborate.

La PIPL prevede, affinché si possano trattare informazioni personali, che alcune condizioni debbano essere soddisfatte. In particolare: deve essere fornito un consenso chiaro ed espresso della persona interessata dal trattamento; tale consenso deve essere dato su base volontaria e previa rappresentazione di tutte le modalità del trattamento; il consenso può essere revocato in qualsiasi momento dalla persona interessata e il titolare del trattamento deve predisporre una modalità di revoca del consenso che sia facilmente accessibile al soggetto i cui dati sono trattati; inoltre, il responsabile del trattamento non può rifiutarsi di fornire prodotti o servizi a chi non ha prestato il proprio consenso, a meno che il trattamento dei dati personali non sia necessario per la fornitura dei suddetti prodotti o servizi.

Con riferimento alle 'informazioni personali sensibili' il PIPL offre un livello di protezione superiore rispetto alle generiche informazioni personali. Le tipologie di dati rientranti in questa categoria sono: i dati biometrici, gli orientamenti religiosi, le informazioni relative allo stato di salute delle persone, le informazioni relative allo stato patrimoniale delle persone e i dati personali dei soggetti minori di 14 anni. Affinché tali informazioni possano essere trattate occorre un consenso rafforzato oltre che una finalità specifica, necessaria e legittima.

CORRADO MORICONI 马思勇

Link al testo originale in cinese della Legge sul sito dell'Assemblea Nazionale del Popolo: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml