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. Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale.

Il 28 settembre 2022 la Commissione europea ha pubblicato due proposte di direttiva che si collocano all'interno di un "pacchetto" di misure atte a sostenere gli obiettivi di "eccellenza e fiducia" relativi all'Intelligenza Artificiale (IA) come già delineati nei precedenti documenti istituzionali dell'Unione. In particolare, tale pacchetto – come si evince dalla relazione di accompagnamento (*Explanatory Memorandum*) – comprende tre linee di intervento tra loro complementari: 1) la proposta di regolamento del 21 aprile 2021 su regole armonizzate e orizzontali sull'Intelligenza Artificiale (*AI Act*) su cui v. la notizia n. 1 del numero 2/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf ; 2) una revisione di norme in tema di sicurezza dei prodotti, tanto settoriali quanto orizzontali; 3) l'armonizzazione di regole di responsabilità civile adeguate alle caratteristiche dei moderni sistemi di Intelligenza Artificiale.

All'interno del terzo filone di interventi citati, la prima proposta stabilisce l'armonizzazione di alcuni profili probatori inerenti ai regimi di responsabilità civile esistenti negli Stati membri e fondati sul criterio della colpa, in modo da garantire che i soggetti danneggiati da un sistema di IA cd. "ad alto rischio" godano di un livello di protezione equivalente a quello di cui godrebbero se i danni in questione fossero stati causati senza il coinvolgimento di un sistema di IA (Considerando n. 7). A tal fine, si prevedono in favore del danneggiato meccanismi di semplificazione probatoria potenzialmente in grado di supplire alle difficoltà generate dalle peculiarità dei sistemi di IA, caratterizzati da funzioni di c.d. auto-apprendimento, nonché da scarsa comprensibilità (opacità) da parte del soggetto danneggiato chiamato a provare in giudizio la condotta colposa del responsabile e il nesso di causalità tra questa e il danno.

La proposta in esame fa seguito, specificamente, alla Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL), già illustrata su questa Rubrica nel numero 4/2020, alla notizia n. 1: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf.

Essa, tuttavia, condivide poco o niente con la proposta del Parlamento europeo. *In primis*, differente è la scelta dello strumento normativo: il regolamento nella Risoluzione, la direttiva nella proposta della Commissione. In secondo luogo, la *AI Liability Directive* propone una forma di armonizzazione dei regimi di responsabilità civile esistenti tra gli Stati membri, mentre la Risoluzione del 2020 elaborava nuove forme di responsabilità *ad hoc* – seppure non limitative di altri regimi di responsabilità esistenti – in capo agli operatori di sistemi di IA, introducendo le nozioni di operatore di *back-end* e di *front-end*. Da ultimo, mentre la proposta di Regolamento prevedeva un regime di responsabilità oggettiva di detti operatori (fondata sul rischio e sul grado di controllo su di esso esercitato da ciascuno), la Commissione ha optato per armonizzare unicamente i regimi di responsabilità per colpa esistenti a livello nazionale, demandando alla futura revisione della direttiva la valutazione intorno all'opportunità di introdurre regimi di responsabilità oggettiva, così come forme di assicurazione obbligatoria.

L'iniziativa, dunque, si propone di completare il quadro di tutele approntate dall'*AI Act*, che prevede l'imposizione di taluni obblighi gravanti *ex ante* su fornitori e utenti di sistemi di IA "ad alto rischio" nella fase di immissione del software sul mercato. La proposta, in questo modo, intende contribuire all'effettività dei suddetti requisiti, poiché la non conformità del sistema di IA agli standard previsti dall'*AI Act* è in grado di attivare *ex post* i meccanismi di alleggerimento probatorio proposti dalla Commissione in caso di verificazione di eventi dannosi causalmente riconducibili al sistema stesso. Il testo si compone di 9 articoli, di cui si espongono di seguito i tratti salienti.

L'art. 1 circoscrive oggetto e scopo della direttiva. Essa stabilisce regole armonizzate in tema di "*disclosure*" di prove per i sistemi di IA ad alto rischio e di onere della prova nei casi di richieste di risarcimento danni proposte davanti ai giudici nazionali a titolo di responsabilità extracontrattuale e fondate sul criterio di imputazione della colpa. Allo stesso tempo, precisa la Commissione, la direttiva non incide: sulle norme del diritto dell'Unione che disciplinano le condizioni di responsabilità nel settore dei trasporti; sui diritti da chiunque azionabili in virtù delle norme nazionali di recepimento della Direttiva 85/374/CEE (cd.

"responsabilità del produttore"); sulle norme nazionali che determinano a chi spetta l'onere della prova, il grado di certezza richiesto in ordine alla stessa, ovvero il modo in cui viene definita la colpa, al di fuori di quanto previsto dagli articoli 3 e 4. Inoltre, agli Stati membri è consentito adottare o mantenere norme nazionali più favorevoli per i danneggiati, purché compatibili con il diritto dell'Unione, dunque anche regimi di responsabilità oggettiva esistenti a livello nazionale e fondati su elementi diversi dal difetto del prodotto (Considerando n. 11).

Dalle definizioni di cui all'art. 2 emerge con tutta evidenza la finalità di coordinamento tra la proposta in esame e la proposta di*AI Act*, il cui contenuto viene richiamato *per relationem* con riguardo alle nozioni di "sistema di IA", "sistema di IA ad alto rischio", "fornitore" e "utente". In aggiunta, viene precisato il significato di alcune locuzioni, tra cui spicca quella di "richiesta di risarcimento" (*claim for damages*), che viene circoscritta al danno causato da un *output* prodotto da un sistema di IA o dall'omissione di tale sistema nel produrre un *output* laddove esso avrebbe dovuto essere prodotto.

Nucleo centrale della proposta sono i sistemi di semplificazione probatoria di cui agli artt. 3 e 4 in favore del danneggiato. All'art. 3 si prevede un meccanismo di cd. "*disclosure*" probatoria, cui consegue eventualmente una presunzione di colpa del fornitore (o di un soggetto a questo equiparato) ovvero dell'utente del sistema di IA. Il giudice nazionale ha il potere di ordinare a tali soggetti di produrre prove relative a specifici sistemi di IA ad alto rischio sospettati di aver causato un danno, purché la relativa richiesta sia proporzionata. La proposta di direttiva non specifica in cosa debbano consistere tali prove, ma prevede che per stabilire se una richiesta di prove sia proporzionata il giudice deve prendere in considerazione i segreti commerciali nel significato di cui all'articolo 2(1) della Direttiva (EU) 2016/943 e le informazioni confidenziali quali le informazioni relative alla sicurezza pubblica o nazionale.. Tale potere è esercitabile dal giudice in un duplice momento: sia in via anticipatoria, qualora cioè venga proposta istanza da un attore "potenziale" (*potential claimant*, ossia che non ha ancora proposto domanda giudiziale), il quale abbia previamente richiesto tale esibizione ai suddetti soggetti senza ottenere riscontro, purché fornisca elementi sufficienti a sostenere la plausibilità della domanda risarcitoria; sia su richiesta dell'attore nel corso di un giudizio già avviato. In questo modo si consente all'attore di ottenere informazioni che devono essere conservate a norma dell'*AI Act*, il quale tuttavia non prevede il corrispondente diritto del danneggiato di accedervi (Considerando 16). Il giudice può anche ordinare la conservazione della prova nei modi che ritenga più consoni.

Qualora il convenuto non ottemperi all'ordine di esibizione o conservazione della prova, scatta la presunzione di inosservanza da parte del convenuto dei doveri di attenzione (*duty of care*) relativi al sistema di IA per cui era stato pronunciato l'ordine, rilevanti a livello nazionale ed europeo, con particolare riferimento ai requisiti posti dall'*AI Act*. La presunzione in esame ha carattere relativo, in quanto è superabile dal convenuto a norma dell'ultimo paragrafo dell'art. 3 fornendo prova contraria (Considerando n. 21, art. 3 par. 5). L'art. 3 delinea, dunque, un regime di responsabilità per colpa di fornitori e utenti per la mancata ottemperanza agli standard posti dall'*AI Act*, la cui prova gravante sul danneggiato viene alleggerita tramite un meccanismo di *disclosure* a carico del convenuto e una eventuale presunzione di colpa del convenuto, che interviene nel caso di sua mancata ottemperanza all'ordine di *disclosure*. Esso contempla solo quei danni che siano la manifestazione di un rischio specificamente contemplato dalla normativa di sicurezza *ex ante* (Considerando 22 e 25).

Il secondo strumento presuntivo, fissato dall'art. 4, concerne il nesso di causalità tra la condotta colposa del convenuto e l'*output* prodotto dal sistema di IA, oppure, secondo il caso, tra la condotta colposa del convenuto e la mancata produzione da parte del sistema di IA dell'*output* che il sistema di IA avrebbe dovuto produrre. Tale presunzione opera, ed è rilevante, subordinatamente all'avverarsi di tutte le seguenti condizioni: a) l'attore ha provato – o il giudice ha presunto ex art. 3 – la colpa del convenuto, consistente nella violazione di un doveri di attenzione (*duty of care*) rilevanti a livello nazionale ed europeo, diretti a prevenire la tipologia di danno occorso; b) si può ritenere ragionevolmente probabile, in base alle circostanze del caso, che la colpa del convenuto abbia influenzato l'*output* generato dal sistema, ovvero la sua mancata produzione; c) l'attore ha provato il nesso di causalità tra il danno subito e l'*output* o la sua mancata produzione da parte del sistema di IA. Il par. 2 dell'art. 4 specifica che la condizione di cui alla lett. a) dovrebbe ritenersi integrata unicamente qualora l'attore abbia dimostrato che il fornitore o l'utente non si sono conformati ai requisiti stabiliti dai capi 2 e 3 del Titolo III dell'*AI Act*. In particolare, si fa riferimento alla inosservanza degli obblighi: a) di

cui all'art. 10, parr. 2-4 dell'*AI Act*, in caso di mancato sviluppo del sistema tramite fasi di addestramento, convalida e test di set di dati che soddisfano i criteri di qualità ivi contenuti; b) di trasparenza (art. 13 *AI Act*); c) di supervisione umana (art. 14 *AI Act*); d) di accuratezza, robustezza e cybersicurezza (artt. 15 e 16 *AI Act*). La norma considera, poi, specificamente i profili di colpa dell'utente, facendo riferimento alla violazione degli obblighi previsti dall'art. 29 dell'*AI Act* (obbligo di utilizzare il sistema secondo le istruzioni per l'uso, obbligo di interrompere l'uso quando necessario, qualora abbia esposto il sistema a *input* rientranti nel suo controllo) e precisando che, qualora si tratti di utente non professionale, la presunzione opera solo se dimostrato che questo abbia concretamente interferito con il funzionamento del sistema. Anche la presunzione di causalità di cui all'art. 4 è superabile dal convenuto, dimostrando, ad esempio, che la sua condotta non può aver cagionato il danno (Considerando n. 30, art. 4 par. 7). Inoltre, la presunzione è preclusa *ab origine* all'attore qualora il convenuto dimostri che la prova di cui è stata ordinata la *disclosure* era facilmente accessibile al danneggiato. Occorre rilevare, infine, che la medesima norma contempla l'ipotesi di danni cagionati da sistemi di IA non ad alto rischio (i quali non sono soggetti ai requisiti obbligatori dell'*AI Act*), prevedendo che la presunzione di causalità debba applicarsi tutte le volte in cui il giudice ritenga eccessivamente complesso per il danneggiato fornire la relativa prova.

Ai sensi dell'art. 5, la Direttiva sarà sottoposta a revisione dopo cinque anni dalla sua entrata in vigore al fine di valutare l'eventuale opportunità di introdurre forme di responsabilità oggettiva e di assicurazione obbligatoria.

TOMMASO DE MARI CASARETO DAL VERME

https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

2. Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE.

La seconda proposta della Commissione in tema di responsabilità civile consiste in una nuova direttiva sulla responsabilità da prodotto difettoso, in sostituzione della Direttiva 85/374/CEE (*Product Liability Directive*: PLD). Essa risponde alla necessità, avvertita dalle istituzioni eurounitarie, di rivedere la vigente PLD alla luce delle moderne evoluzioni della tecnologia, con particolare riguardo ai sistemi di IA. Tali istanze sono emerse, da ultimo, tanto nella citata Risoluzione del Parlamento europeo del 20 ottobre 2020 (su cui v. su questa Rubrica la notizia n. 1 nel numero 4/2020: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf), quanto nella successiva valutazione di impatto (*Inception Impact Assessment)* della Commissione del 30 giugno 2021 intitolata "*Adapting liability rules to the digital age and circular economy*" (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en).

In particolare, il Parlamento, pur rilevando la generale adeguatezza della direttiva ad affrontare i danni cagionati da *smart products*, sottolineava in quella risoluzione la necessità di adeguare alcune nozioni in essa contenute – tra cui "prodotto", "difetto" e "produttore" – alla più recente evoluzione tecnologica, nonché di considerare l'inversione dell'onere della prova per i danni causati dalle tecnologie digitali emergenti in casi chiaramente definiti e previa un'adeguata valutazione. La Commissione, a sua volta, nella citata valutazione di impatto, suggeriva di estendere il regime di responsabilità oggettiva in questione anche ai prodotti immateriali (ad es. contenuti digitali e software), nonché ai difetti risultanti da modifiche subite dai prodotti dopo la loro immissione sul mercato (ad es. aggiornamenti del software), ai difetti risultanti da interazioni con altri prodotti e servizi (ad es. IoT) ed ai rischi ricollegati alla connettività ed alla cybersicurezza. Inoltre, la Commissione proponeva di alleggerire l'onere della prova gravante sul consumatore-danneggiato, invertendo l'onere della prova e precludendo al convenuto la prova liberatoria del cd. "rischio da sviluppo" nei casi di danni cagionati da sistemi di IA con funzioni di c.d. auto-apprendimento e adattamento.

La proposta in esame intende completare la tutela approntata dalla *AI Liability Directive* (su cui v. la notizia precedente in questo numero di questa Rubrica), la quale, se introduce un regime "semplificato" di responsabilità degli operatori di sistemi di IA ad alto rischio, considera tuttavia solo i regimi di responsabilità extracontrattuale per colpa e, peraltro, non contempla tutti i rischi derivanti dalla produzione e dall'utilizzo di *smart products*, ma solo quelli ricollegati ai requisiti posti dalla

normativa di sicurezza *ex ante*. Il sistema della responsabilità da prodotto difettoso, invece, attribuisce al danneggiato una forma di tutela più ampia, in quanto prescinde dalla colpa del produttore e consente di considerare difettoso anche un prodotto conforme alle norme di sicurezza. La complessità che caratterizza le moderne tecnologie (non solo di IA, ma anche i nuovi modelli di business dell'economia circolare e le nuove *supply chain* globali) pone, tuttavia, i suddetti interrogativi circa la perdurante efficienza e operatività della vigente PLD, cui la proposta della Commissione tenta di fornire una prima risposta. La proposta si compone di venti articoli suddivisi in quattro capi. Di seguito si espongono le principali novità rispetto alla normativa vigente.

L'art. 4 fornisce una vasta gamma di definizioni che vogliono rispecchiare l'evoluzione tecnologica in ambito digitale. In particolare, alla definizione di «prodotto» di cui all'art. 2 della vigente PLD si aggiungono i *file* di produzione digitale ("*digital manufacturing file*", ossia una versione digitale o un modello digitale di un bene mobile) e i *software*. Similmente, la nozione di «componente» include qualsiasi bene, materiale o immateriale, o qualsiasi servizio correlato, integrato o interconnesso con un prodotto. Il novero dei danni risarcibili viene ampliato, comprendendo, oltre alla morte, alle lesioni personali e ai danni a cose diverse dal prodotto stesso (art. 9 della proposta di nuova PLD): i danni alla salute psicologica medicalmente accertabili; il danneggiamento o la distruzione di qualsiasi bene, eccetto un prodotto danneggiato da una componente difettosa dello stesso e beni utilizzati per scopi professionali; la perdita o il danneggiamento di dati non utilizzati esclusivamente a fini professionali.

La definizione di «prodotto difettoso» di cui all'art. 6 della vigente PLD viene arricchita e maggiormente specificata dall'art. 6 della proposta. Un prodotto è difettoso quando non offre la sicurezza che la generalità dei consociati o il "grande pubblico" ("*public at large*") può legittimamente attendersi. Nel memorandum di accompagnamento della proposta, si trova scritto che il relativo test è sostanzialmente lo stesso di quello richiesto dalla vigente PLD, ma che, per tener conto della natura dei prodotti nell'era digitale e per riflettere la giurisprudenza della Corte di Giustizia dell'Unione Europea, alcuni fattori sono stati aggiunti alla lista non esaustiva dei fattori di cui i giudici devono tener conto nell'accertare la difettosità, tra cui l'interconnessione e le funzioni di auto-apprendimento. In particolare, le circostanze di cui tenere conto, tra le altre, ai fini della valutazione intorno alla difettosità del prodotto ora includono: a) nella presentazione del prodotto, le istruzioni per l'installazione, l'uso e la conservazione del prodotto; b) l'uso corretto o distorto ragionevolmente prevedibile; c) gli effetti sul prodotto causati dalla sua abilità di apprendere successivamente al rilascio sul mercato; d) gli effetti causati sul prodotto da altri prodotti con cui esso entra in contatto; e) oltre al momento della messa in circolazione del prodotto, anche quello in cui il produttore perde il controllo sullo stesso qualora questo perduri anche successivamente al rilascio; f) i requisiti di sicurezza del prodotto, compresi quelli di cybersicurezza; g) qualsiasi intervento di un'autorità di regolazione o di un operatore economico di cui all'articolo 7 relativo alla sicurezza dei prodotti; h) le aspettative dello specifico utente finale cui il prodotto è destinato. Infine, la regola per cui la sola esistenza di un prodotto più evoluto non può rendere il prodotto difettoso include ora anche gli aggiornamenti dello stesso.

Maggiormente dettagliata è la nozione di «produttore» fornita dall'art. 7 della proposta di nuova PLD, con cui la Commissione si preoccupa, in particolare, di specificare la responsabilità solidale del produttore della singola componente difettosa, così come la responsabilità dell'importatore nel caso in cui il produttore sia stabilito al di fuori dell'Unione.

All'art. 8 della proposta di nuova PLD è previsto un meccanismo di *disclosure* simile a quanto visto nella coeva proposta di *AI Liability Directive* (su cui v. notizia precedente in questo numero di questa Rubrica), impiegabile unicamente nel corso del giudizio e purché l'attore abbia fornito elementi sufficienti a fondare la plausibilità della propria domanda risarcitoria. La mancata ottemperanza all'ordine attiva, anche in questo caso, una presunzione (relativa) che, però, concerne la prova del difetto. All'art. 9 della proposta di nuova PLD, infatti, l'onere della prova gravante sul danneggiato rimane invariato rispetto alla vigente PLD, tuttavia con l'aggiunta che il prodotto si presume difettoso se, alternativamente: a) il produttore non abbia ottemperato all'ordine di *disclosure*; b) l'attore dimostri che il prodotto non è conforme a standard di sicurezza obbligatori che ricomprendono la stessa tipologia di rischio di cui al danno occorso; ovvero c) l'attore provi un palese malfunzionamento del prodotto durante un impiego normale dello stesso.

La medesima norma stabilisce che si presume anche il nesso di causalità tra difetto e danno, ove sia accertato il difetto del prodotto e la compatibilità

tra la natura del danno cagionato e il difetto in questione. In ogni caso, il giudice, qualora constati una eccessiva complessità probatoria gravante sul danneggiato, può presumere il difetto e il nesso di causalità qualora il danneggiato abbia fornito elementi sufficienti a provare che il prodotto ha contribuito alla verificazione del danno e che è probabile che il prodotto fosse difettoso o che la difettosità sia stata causa probabile del danno. Con tale disposizione viene positivizzata un'istanza di tutela avanzata da più parti (soprattutto in dottrina), tesa a valorizzare il fattore della "verosimiglianza" con riguardo alla prova del difetto (e non limitato alla prova liberatoria del "difetto sopravvenuto").

L'art. 10 della proposta di nuova PLD in tema di esclusione della responsabilità ripercorre quasi pedissequamente quanto previsto dall'art. 7 della vigente PLD, ma articola le prove liberatorie in rapporto alle rinnovate categorie di soggetti responsabili. Particolare rilievo assume la circostanza per cui l'applicazione del "rischio da sviluppo" (lett. f) viene limitata al produttore, precludendo dunque all'importatore e al distributore di avvalersene. Costituisce assoluta novità, invece, quanto previsto dal secondo paragrafo dell'art. 10 della proposta di nuova PLD, che esclude l'esenzione da responsabilità per il cd. "difetto sopravvenuto" previsto dalla lettera *c*) del par. 1 del medesimo articolo, qualora il difetto, in costanza di possibilità di controllo da parte del fabbricante, sia causato da: a) un servizio correlato; b) il software, inclusi i suoi aggiornamenti; c) la mancanza di aggiornamenti ove necessari per garantire la sicurezza del prodotto.

Sostanzialmente invariati rimangono i termini di prescrizione e decadenza di cui alla vigente PLD. Degna di nota è, infine, la disposizione dell'art. 3 della proposta di nuova PLD sul livello di armonizzazione della Direttiva, che preclude agli Stati membri di mantenere o introdurre disposizioni divergenti da quelle stabilite nella proposta, comprese disposizioni più o meno rigorose per conseguire un diverso livello di protezione dei consumatori, salvo diversa disposizione della direttiva stessa. Tale previsione, assente nella versione vigente della direttiva, appare tesa a neutralizzare lo spazio di discrezionalità che la vigente PLD aveva concesso agli Stati nel suo recepimento - specialmente con riguardo alla prova del rischio da sviluppo (art. 15, lett. b) della vigente PLD) – e che spesso è stata additata come responsabile di un sostanziale fallimento nell'armonizzazione del livello di tutela dei consumatori danneggiati nel territorio dell'Unione.

TOMMASO DE MARI CASARETO DAL VERME

https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en

3. Proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act): First Presidency compromise text del 12 luglio 2022.

Il 12 luglio 2022, a seguito di un lungo *iter* iniziato lo scorso 23 febbraio 2022 e sulla base dei suggerimenti forniti dagli Stati membri, la Presidenza del Consiglio dell'Unione Europea ha redatto un primo (parziale) *compromise text* della proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo ("**Proposta di Data Act**" o "**DA**"; v. notizia n. **4** sul numero **1/2022** di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf). Il *compromise text* concerne i soli Capi I, II, III e IV della Proposta di Data Act e i relativi Considerando.

Dalle modifiche effettuate dalla Presidenza del Consiglio al **Capo I** del DA emerge, anzitutto, che essa si occupa di stabilire non solo, come già indicato nella originaria proposta della Commissione, "*norme armonizzate relative alla messa a disposizione dei dati generati dall'uso di un prodotto o di un servizio correlato all'utente di tale prodotto o servizio, alla messa a disposizione di dati da parte dei titolari dei dati ai destinatari dei dati, alla messa a disposizione di dati da parte dei titolari dei dati agli enti pubblici o alle istituzioni, agenzie o organismi dell'Unione, a fronte di necessità eccezionali, per l'esecuzione di un compito svolto nell'interesse pubblico*", bensì anche quelle relative "*alla facilitazione del passaggio da un servizio di trattamento dei dati all'altro, all'introduzione di garanzie contro l'accesso illegale di terzi ai dati non personali e allo sviluppo di standard di interoperabilità per i dati da trasferire e utilizzare*" (art. 1 (1) DA).

Il nuovo paragrafo (1a) dell'art. 1 chiarisce, ora, che il DA riguarda "*dati personali e non personali, compresi i seguenti tipi di dati o nei seguenti contesti: (a) il Capo II si applica ai dati relativi alle prestazioni, all'uso e all'ambiente dei prodotti e dei servizi correlati; (b) il Capo III si applica a tutti i dati del settore privato soggetti agli obblighi di condivisione dei dati previsti dalla legge; (c) il Capo IV si applica a tutti i dati del settore privato a cui si accede e che vengono utilizzati sulla base di accordi contrattuali tra aziende; (d) il Capo V si*

applica a tutti i dati del settore privato con particolare attenzione ai dati non personali; (e) il Capo VI si applica a tutti i dati trattati dai servizi di elaborazione dati; (f) il Capo VII si applica a tutti i dati non personali conservati nell'Unione da fornitori di servizi di elaborazione dati".

Mediante alcune modifiche all'art. 1(2), il *compromise text* presidenziale meglio illustra l'ambito territoriale di applicazione della Proposta di Data Act, stabilendo che con riguardo ai fabbricanti di prodotti e ai fornitori dei servizi immessi nel mercato dell'Unione, nonché ai titolari dei dati che mettono dati a disposizione dei destinatari dei dati nell'Unione, il DA si applica indipendentemente dal loro luogo di stabilimento. Il principio di irrilevanza del luogo di stabilimento trova ora applicazione anche in relazione ai fornitori di servizi di trattamento dei dati che offrono tali servizi a clienti nell'Unione.

I paragrafi (3), (4) e (4a) dell'art. 1 del DA – a seguito delle recenti modifiche – chiariscono, invece, il rapporto della Proposta di Data Act con la restante disciplina vigente; in particolare, stabiliscono che la proposta in commento non pregiudica l'applicazione del GDPR (e dell'ulteriore disciplina in materia di protezione dei dati personali, della privacy e della riservatezza delle comunicazioni e dell'integrità delle apparecchiature terminali) e del regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali nell'Unione.

Il *compromise text* presidenziale ha aggiunto, inoltre, alcune definizioni all'art. 2 del DA – tra le quali quella di 'dato personale' e 'dato non personale', nonché di 'consenso' e 'interessato' – effettuando un semplice richiamo a quelle fornite dall'art. 4 del GDPR (v. art. 2, nn. 1a, 1ab, 1ac e 1ad DA); altre definizioni di cui al medesimo art. 2 sono state, invece, solamente in parte modificate. Tra queste, rivestono un rilievo cruciale ai fini del regolamento quelle di:

- 'prodotto': "*un bene materiale che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati tramite un servizio di comunicazione elettronica accessibile al pubblico e la cui funzione primaria non è la conservazione e il trattamento dei dati né è progettato principalmente per visualizzare o riprodurre contenuti, o per registrare e trasmettere contenuti*" (art. 2, n. 2 DA);
- 'servizio correlato': "*un servizio digitale, anche software, che al momento dell'acquisto, dell'affitto o del contratto di noleggio è interconnesso con un prodotto in modo tale che la sua assenza impedirebbe al prodotto di svolgere una delle sue funzioni*" (art. 2, n. 3 DA);
- 'assistenti virtuali': "*un software che può elaborare richieste, compiti o domande, incluse quelle basate su input sonori o scritti, gesti o movimenti, e che, sulla base di tali richieste, compiti o domande, fornisce accesso ad altri servizi o controlla dispositivi fisici collegati*" (art. 2, n. 4 DA);
- 'utente': "*una persona fisica o giuridica, incluso un interessato, che possiede, affitta o noleggia un prodotto o riceve un servizio correlato*" (art. 2, n. 5 DA);
- 'titolare dei dati': "*una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale di attuazione del diritto dell'Unione, o, nel caso di dati non personali e attraverso il controllo della progettazione tecnica del prodotto e dei servizi correlati, la capacità di mettere a disposizione determinati dati*" (art. 2, n. 6 DA).

Il *compromise text* ha poi previsto una modifica alla rubrica del **Capo II** del DA, che ora è intitolato "*Diritto degli utenti di utilizzare i dati dei prodotti connessi e dei servizi correlati*", al fine di riflettere in modo più preciso gli obiettivi del Capo in parola.

L'art. 3 del DA, all'esito delle modifiche effettuate dalla Presidenza del Consiglio dell'UE, ora dispone – innanzitutto – che i prodotti devono progettati e fabbricati, e i servizi correlati forniti, in modo tale che i dati generati dal loro uso che sono accessibili al titolare dei dati siano, per impostazione predefinita e gratuitamente, facilmente, in maniera sicura e, ove pertinente e opportuno, accessibili all'utente in un formato strutturato, comunemente utilizzato e leggibile a macchina (art. 3(1) DA); in secondo luogo, che prima di concludere un contratto di acquisto, affitto o noleggio di un prodotto o di un servizio correlato, il titolare dei dati deve fornire (almeno) una serie di informazioni indicate all'art. 3(2) del DA.

L'art. 4(1) del DA – così come risultante dalle modifiche del *compromise text* – stabilisce, invece, che qualora l'utente non possa accedere direttamente ai dati a partire dal prodotto o dal servizio correlato, il titolare dei dati deve comunque mettere a disposizione dell'utente i dati generati dall'utilizzo del prodotto o del servizio correlato che sono accessibili al medesimo titolare (oltre ai i metadati rilevanti), senza indebito ritardo, gratuitamente, facilmente, in maniera sicura, in un

formato strutturato, comunemente utilizzato e leggibile a macchina e, ove applicabile, in modo continuo e in tempo reale. Ciò dovrà avvenire sulla base di una semplice richiesta mediante mezzi elettronici, ove tecnicamente fattibile.

Ai sensi dell'art. 4(2)-(6) del DA, resta fermo che: *1)* il titolare dei dati non può imporre all'utente di fornire informazioni al di là di quanto necessario per verificare la sua qualifica e che il titolare non potrà conservare informazioni relative all'accesso dell'utente ai dati richiesti; *2)* come stabilito al nuovo punto 2a, il titolare dei dati non deve costringere, ingannare o manipolare in alcun modo l'utente sovvertendo o compromettendo l'autonomia, il processo decisionale o le scelte di questo al fine di ostacolarne l'esercizio del diritto di accesso; *3)* i segreti commerciali sono comunicati solo a condizione che siano adottate in anticipo tutte le misure specifiche necessarie per tutelarne la riservatezza; *4)* l'utente non può utilizzare i dati ottenuti per sviluppare un prodotto in concorrenza con quello da cui provengono i dati; *5)* come stabilito al nuovo punto 5a, l'utente non deve ricorrere a mezzi coercitivi o abusare di evidenti lacune nell'infrastruttura tecnica del titolare dei dati al fine di ottenere l'accesso ai dati; *6)* qualora l'utente non sia l'interessato cui si riferiscono i dati personali richiesti, i dati personali generati dall'uso di un prodotto o di un servizio correlato sono messi a disposizione dell'utente dal titolare dei dati solo se esiste una base giuridica valida a norma dell'articolo 6, paragrafo 1, del GDPR; *7)* il titolare dei dati potrà utilizzare i dati non personali generati dall'uso di un prodotto o di un servizio correlato solo sulla base di un accordo contrattuale con l'utente, mai però al fine di ottenere informazioni sulla situazione economica, sulle risorse e sui metodi di produzione o sull'utilizzo da parte dell'utente che potrebbero compromettere la sua posizione commerciale nei mercati in cui l'utente è attivo.

L'art. 5 del DA, che regola il diritto dell'utente di condividere i dati con terzi, stabilisce ora il necessario rispetto di alcune condizioni che riproducono, in buona sostanza, quelle già previste dall'art. 3. Mentre, sono state apportate alcune modifiche all'art. 6 del DA al fine di disciplinare il possibile scenario in cui l'utente non coincida con l'interessato, non previsto nell'originaria proposta della Commissione europea.

All'art. 7 del DA, infine, è stato precisato che gli obblighi di cui al Capo II non si applicano neppure ai "*dati generati dall'uso di prodotti fabbricati o di servizi correlati forniti da imprese che si qualificano come medie imprese*" (art. 7(1) DA).

Il titolo del **Capo III** è stato poi modificato in "*Obblighi orizzontali per i titolari di dati tenuti per legge a mettere a disposizione i dati nei rapporti tra imprese*", al fine di rendere chiaro che gli obblighi ivi contenuti sono di natura orizzontale.

Il *compromise text* ha previsto poi alcune modifiche all'art. 8 del DA, al fine di alleggerire il linguaggio della originaria Proposta di Data Act, per non imporre in capo al titolare dei dati l'onere (eccessivamente gravoso) di dimostrare che non vi è stata discriminazione del destinatario dei dati. La disposizione in parola, infatti, ora prevede semplicemente che "*il titolare dei dati dovrà senza indebito ritardo fornire al destinatario dei dati, su richiesta di questo, informazioni che dimostrino l'assenza di discriminazioni*". Inoltre, è stato chiarito che non è richiesto al titolare dei dati di condividere segreti commerciali con il destinatario dei dati, a meno che ciò non sia previsto dalla legge.

All'art. 9(2), invece, è stato chiarito che – come anche indicato all'art. 7(1) del DA – quando il destinatario sia una micro, piccola o media impresa, i principi sanciti nella Proposta di Data Act in relazione a tali tipologie di imprese valgono a condizione che esse non abbiano imprese connesse o collegate, secondo la definizione di cui all'articolo 3 dell'allegato alla raccomandazione 2003/361/CE, che non si qualifichino come micro, piccole o medie imprese.

All'art. 10 del DA – che disciplina il meccanismo di risoluzione delle controversie tra titolari dei dati e destinatari di questi – è stato aggiunto il nuovo paragrafo (7a), con il quale si è previsto che "[g]*li organi di risoluzione delle controversie rendono pubbliche le relazioni annuali di attività*" e che il "*rapporto annuale comprende in particolare le seguenti informazioni: (a) il numero delle controversie decise; (b) il risultato di tali controversie; (c) il tempo medio richiesto al fine di risolvere tali controversie; (d) problemi comuni che si verificano frequentemente e che portano a controversie tra le parti; tali informazioni possono essere accompagnate da raccomandazioni su come evitare o risolvere tali problemi, al fine di facilitare lo scambio di informazioni e di migliori pratiche*".

L'articolo 11(2) del DA è stato, invece, modificato per tenere meglio conto di ciò che dovrebbe accadere in caso di utilizzo o divulgazione non autorizzati dei dati; mentre, è stato aggiunto l'art. 11(2a) al fine di estendere le salvaguardie di cui all'art. 11(2) anche agli utenti, qualora il destinatario dei dati abbia violato quanto previsto all'art. 6(2)(a) ovvero all'art. 6(2)(b) della Proposta di Data Act.

Il **Capo IV** del DA, ora rinominato "*Clausole contrattuali abusive relative all'accesso ai dati e al*

relativo utilizzo", non presenta invece novità di rilievo rispetto all'originaria proposta della Commissione, salvo un coordinamento con l'art. 7(1) – simile a quello di cui all'art. 9(2) – che chiarisce la sfera di applicabilità delle disposizioni racchiuse in tale articolo alle micro, piccole o medie imprese.

RICCARDO ALFONSI

https://data.consilium.europa.eu/doc/document/ST-11194-2022-INIT/en/pdf

4. La proposta di Regolamento UE sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (c.d. Cyber Resilience Act)

Il 15 settembre 2022 la Commissione europea ha presentato, con la comunicazione n. 454, il progetto di Reg. UE in materia di cibersicurezza per i prodotti digitali, c.d. *Cyber Resilience Act* (nel prosieguo, "proposta di regolamento" o "Cyber Resilience Act").

Alla base della proposta di regolamento è il crescente numero di attacchi informatici che hanno raggiunto un costo globale di 5.5 trilioni nel 2021. Ciò sarebbe da ricondurre essenzialmente a due fattori: *a*) un livello di sicurezza informatica generalmente basso, dovuto in parte alle insufficienze degli aggiornamenti; *b*) una scarsa alfabetizzazione digitale dell'utenza, che ostacola la scelta consapevole dei prodotti e il loro uso prudente. Inoltre, in ambienti interconnessi, gli incidenti riguardanti il singolo prodotto possono propagarsi con estrema rapidità, causando gravi interruzioni delle attività economiche e sociali o, financo, mettendo a rischio la vita umana. La dimensione globale dei mercati dei prodotti con elementi digitali, poi, comporta che la maggior parte di essi non sono attualmente soggetti ad alcuna regolazione europea sulla sicurezza informatica. È il caso, in particolare, dei *software* non incorporati, sovente bersaglio di attacchi di rilevante entità.

Come esplicitato nella comunicazione della Commissione "*Plasmare il futuro digitale dell'Europa"* del 19 febbraio 2020 (COM (2020) 67 definitivo), la cybersicurezza è uno dei quattro pilastri – oltre alla protezione dei dati, ai diritti fondamentali e alla sicurezza (dei prodotti) – per una società digitale in cui l'innovazione sia promossa entri confini sicuri ed etici.

Per tali ragioni, i due obiettivi principali della proposta di regolamento sono: creare le condizioni affinché siano sviluppati prodotti digitali la cui sicurezza perduri lungo tutto il loro ciclo di vita e promuovere la sicurezza informatica come elemento chiave per la scelta e l'utilizzo di prodotti digitali (v. Considerando 2). Da questi, si diramano quattro obiettivi specifici: *i*) assicurare un'implementazione degli standard di sicurezza sin dalla fase di progettazione e sviluppo; *ii*) fornire un quadro legislativo coerente in materia, per agevolare la conformità; *iii*) promuovere la trasparenza; *iv*) consentire alle imprese e ai consumatori di utilizzare i prodotti con elementi digitali in modo sicuro (v. Considerando 8).

L'intervento si impone anche in considerazione della frammentarietà e della lacunosità del quadro legislativo esistente. La frammentarietà è data dall'assommarsi delle dir. nn. 2013/40/UE (relativa agli attacchi contro i sistemi di informazione), 2016/1148/UE (c.d. NIS, sulla sicurezza delle reti e dei sistemi informativi), la futura Dir. NIS II e il Reg. 2019/881/UE (relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione) (v. Considerando 4). La lacunosità deriva dall'assenza di prescrizioni specifiche per la sicurezza dei prodotti con elementi digitali, solo episodicamente contemplate da alcune discipline speciali (v. Considerando 3). Lungo tali direttrici, la proposta si coordina coi regimi in vigore, inglobando l'ambito di applicazione materiale del Reg. 2022/30/UE e stabilendo requisiti essenzialmente riproduttivi degli elementi cui all'art. 3, par. 3, lett. *d*), *e*), *f*) della dir. 2014/53/UE.

Ciò premesso, sul piano contenutistico la proposta si compone di 71 Considerando e di 57 articoli, distribuiti lungo 8 Capitoli.

Il Capitolo I delimita anzitutto l'oggetto (art. 1), che si articola in: *a*) norme per l'immissione sul mercato di prodotti con elementi digitali, al fine di garantirne la cybersicurezza; *b*) requisiti essenziali di progettazione, sviluppo e produzione e relativi obblighi per gli operatori economici *c*) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai produttori per garantire la sicurezza informatica dei prodotti con elementi digitali durante l'intero ciclo di vita e relativi obblighi per gli operatori economici; *d*) norme sulla sorveglianza del mercato e sull'applicazione della disciplina in oggetto.

Quanto all'ambito applicativo (art. 2), il regolamento dovrà applicarsi a tutti i prodotti con elementi digitali il cui uso previsto o

ragionevolmente prevedibile include una connessione logica o fisica diretta o indiretta di dati a un dispositivo o a una rete. Ai sensi dell'art. 3, parr. 10 e 11, per "connessione logica" si intende una rappresentazione virtuale di una connessione dati implementata attraverso un'interfaccia *software*; la "connessione fisica", invece, è definita come qualsiasi connessione tra sistemi informativi elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche o meccaniche, fili o onde radio. Restano esclusi i prodotti disciplinati dal Reg. 2017/745/UE (relativo ai dispositivi medici), dal Reg. 2017/746/UE (relativo ai dispositivi medico-diagnostici *in vitro*), poiché prevedono entrambi requisiti relativi ai dispositivi, anche per quanto riguarda il *software*, e obblighi generali per i fabbricanti che riguardano l'intero ciclo di vita dei prodotti, nonché procedure di valutazione della conformità (v. Considerando 14). Inoltre, la proposta non si applicherà ai prodotti con elementi digitali certificati in conformità al Reg. 2018/1139/UE (recante norme comuni in materia di aviazione civile) né a quelli ai cui fa riferimento il Reg. 2019/2144/UE (sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada). Sono sottratti al regime in oggetto anche i prodotti sviluppati esclusivamente per scopi di sicurezza nazionale o militari e quelli specificamente progettati per elaborare informazioni classificate. Da ultimo, la promozione della ricerca e dell'innovazione dovrebbe portare a escludere dal perimetro tracciato anche i *software* liberi e *open-source* sviluppati o forniti al di fuori di un'attività commerciale, e in particolari quelli condivisi apertamente e liberamente accessibili, utilizzabili, modificabili e ridistribuibili (Considerando 10).

Il combinato disposto degli artt. 4 e 5 testimonia la linea di politica del diritto seguita: premessa la libera circolazione dei prodotti con elementi digitali, si prescrivono una serie puntuale di requisiti essenziali per la conformità (Sez. I, All. I) di questi e dei relativi processi messi in atto dai produttori (Sez. II, All. I).

Un regime di maggior rigore è approntato all'art. 6 per i prodotti con elementi digitali assunti come critici, ossia quelli elencati all'All. III e *ivi* suddivisi in due classi di rischio crescenti, a seconda dell'impatto delle potenziali vulnerabilità sul piano della cybersicurezza (v. Considerando 26). Alla Commissione è conferito il potere di modificare la lista, includendo categorie nuove e/o eliminandone alcune, entro parametri predeterminati. I prodotti critici con elementi digitali sono soggetti alle procedure di valutazione di conformità di cui all'art. 24, par. 2 e 3. Alla Commissione è inoltre conferito il potere di adottare atti delegati integrativi, specificando le classi di prodotti altamente critici per i quali i produttori, per dimostrare la conformità all'All. I, sono obbligati al previo ottenimento del certificato europeo di cui al Reg. 2019/881/UE.

Infine, va evidenziato il raccordo con l'attuale quadro normativo europeo relativo ai prodotti (v. Considerando 16) e con le proposte legislative, come l'*Artificial Intelligence Act* (21.4.2021 COM (2021) 206 final). In linea con le indicazioni generali dei Considerando 14 e 29, i prodotti con elementi digitali classificati come sistemi di IA ad alto rischio *ex* art. 6 AIA, che rientrano nell'ambito di applicazione della proposta in analisi e soddisfano i requisiti essenziali di cui alle Sez. I e II dell'All. I, sono considerati conformi ai requisiti relativi alla sicurezza informatica di cui all'art. 15 AIA e seguono la procedura di cui all'art. 43 AIA (art. 8).

Snodo centrale del progetto di regolamento è, senza dubbio, il Capitolo II. Esso condensa una serie di obblighi prescritti agli operatori economici – produttori, rappresentanti autorizzati, importatori, distributori o qualsiasi altra persona fisica o giuridica soggetta agli obblighi stabiliti dal regolamento (art. 3, n. 17) – graduati secondo la loro allocazione nella catena di fornitura e le loro conseguenti responsabilità. A livello generale, i prodotti con elementi digitali possono essere immessi sul mercato solo se forniti in modo corretto, opportunamente installati, sottoposti a manutenzione e utilizzati per lo scopo previsto o in condizioni ragionevolmente prevedibili.

Più precisamente, ai sensi dell'art. 10 della proposta i produttori devono garantire che la progettazione, lo sviluppo e la produzione sia conforme ai requisiti essenziali di cui alla Sez. I dell'All. I, effettuando una previa valutazione individuale dei rischi di cybersicurezza e tenendo conto dei relativi risultati nelle fasi descritte. Particolare importanza rivestono gli obblighi di documentazione: tutti i dati pertinenti o i dettagli dei mezzi utilizzati per garantire che il prodotto e i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'All. I, oltre agli esiti delle verifiche anzidette, sono da includere nella documentazione tecnica *ex* art. 23, che deve precedere l'immissione sul mercato. Inoltre, va documentato sistematicamente qualsiasi aspetto rilevante di cybersicurezza relativo al prodotto, provvedendo, ove le risultanze lo richiedano, ad aggiornare la valutazione di rischio. Tra gli

adempimenti, spicca poi l'esecuzione delle procedure di valutazione della conformità, di cui all'art. 24, che, ove concluse con esito positivo, consentono di redigere la dichiarazione di conformità CE (art. 20) e l'apposizione della relativa marcatura (art. 22). Seguono poi i doveri informativi: le informazioni e le istruzioni di cui all'All. II accompagnano costantemente il prodotto e devono essere chiare, comprensibili, intellegibili e leggibili. Tutti i dati e i documenti necessari a dimostrare la conformità ai requisiti essenziali di cui all'All. I devono essere forniti all'autorità di vigilanza del mercato, su richiesta motivata di essa. Completano il quadro gli obblighi di comunicazione. Ai sensi dell'art. 11 della proposta di regolamento, i produttori devono notificare all'ENISA, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne hanno conoscenza, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali e qualsiasi incidente che possa minarne la sicurezza. Degli incidenti, nonché delle eventuali misure correttive esperibili, deve essere prontamente informata anche l'utenza.

Le obbligazioni dei rappresentanti autorizzati, nominati dal fabbricante mediante mandato scritto, sono assai più ridotte, e il legislatore si premura vieppiù di attribuire ad essi una posizione di interlocutore qualificato dell'autorità di vigilanza del mercato (art. 12).

Agli importatori è affidato, dall'art. 13 della proposta di regolamento, un ruolo – per così dire – di controllo e garanzia. Essi, per prima cosa, sono tenuti a immettere sul mercato solo prodotti con elementi digitali conformi ai requisiti essenziali di cui alla Sez. I dell'All. I e i cui processi messi in atto dal produttore sono conformi ai requisiti essenziali di cui alla Sez. II dell'All. I. Prima dell'immissione sul mercato, tali soggetti devono garantire l'esatta esecuzione delle procedure di valutazione della conformità *ex* art. 24, la redazione della documentazione tecnica e l'apposizione della marcatura CE di cui all'art. 22, assieme alle informazioni e dalle istruzioni di cui all'All. II., da parte del fabbricante. Qualora l'importatore abbia fondati motivi di dubbio sulla conformità del prodotto o dei processi, gli è fatto divieto di immetterlo fino a quando entrambi sono resi conformi. Ove tale diagnosi sopravvenga all'immissione sul mercato, è prescritta l'adozione delle misure correttive necessarie o, se del caso, il richiamo o il ritiro del prodotto. Da ultimi, vanno menzionati i doveri di segnalazione delle vulnerabilità rilevate al fabbricante e a questi e all'autorità di vigilanza del mercato degli Stati membri presso cui il prodotto è stato messo in circolazione, ove si tratti di rischi significativi per la sicurezza informatica.

La platea dei destinatari qualificati termina con i distributori, la cui posizione testimonia un incremento dei doveri di controllo e garanzia proporzionale all'allungamento della catena. A fronte di un generico obbligo di agire con la dovuta attenzione in relazione ai requisiti prescritti, tali operatori sono tenuti, prima della messa a disposizione di un prodotto con elementi digitali, a verificare la sussistenza del marchio CE e l'effettivo assolvimento da parte del produttore e dell'importatore degli adempimenti previsti, rispettivamente, dagli artt. 10, par. 10 e 11, e 13, par. 4. Per il resto, l'art. 14 ricalca fedelmente la disciplina predisposta per gli importatori alla disposizione precedente, quanto ai fondati motivi di dubbio sulla conformità, originari o sopravvenuti, ai doveri di avviso, correzione e intervento.

Merita, infine, segnalare che gli importatori e i distributori sono equiparati ai produttori, con conseguente soggezione alle prescrizioni *ex* artt. 10 e 11, par. 1, 2, 4 e 7, qualora immettano sul mercato un prodotto con elementi digitali con il proprio nome o marchio o vi effettuino una modifica sostanziale (art. 15; cfr. Considerando 24). Solo in quest'ultimo caso, l'estensione comprende anche gli operatori economici non qualificati, ossia, in generale, qualunque persone fisica o giuridica (art. 16).

Il Capitolo III della proposta di regolamento è dedicato alla conformità e si apre, all'art. 18, con un'importante regola presuntiva. Anzitutto, i prodotti con elementi digitali conformi agli *standard* europei armonizzati o a parti di essi si presumono conformi ai requisiti essenziali richiesti dall'All. I della proposta. Altrettanto vale per i prodotti e i processi digitali conformi alle specifiche comuni di cui all'art. 19 o per i quali è stata rilasciata una dichiarazione di conformità UE o un certificato emesso nell'ambito di un sistema europeo di certificazione della cybersicurezza ai sensi del Reg. 2019/881/UE, limitatamente alle caratteristiche *ivi* contemplate (v. Considerando 39). Giova, inoltre, segnalare che: *i*) le evocate specifiche comuni *ex* art. 19 assumono una veste essenzialmente suppletiva, potendo essere adottate dalla Commissione mediante atti di esecuzione se le norme armonizzate non esistono o sono insufficienti, se vi sono ritardi ingiustificati nella procedura di standardizzazione o se la richiesta della Commissione non è stata accettata dalle organizzazioni europee di standardizzazione; *ii*) la dichiarazione di conformità UE segue il modello di

cui all'All. IV, contiene gli elementi specificati nelle pertinenti procedure di valutazione della conformità di cui all'Allegato VI, va sottoposta ad aggiornamento costante e, soprattutto, comporta per il produttore l'assunzione della responsabilità sulla conformità del prodotto (art. 20); *iii*) il marchio CE va apposto in modo visibile, leggibile e indelebile sul prodotto con elementi digitali o, se ciò non è possibile o non può garantirsi, sull'imballaggio e sulla dichiarazione di conformità UE o su di essa e sul sito web per i prodotti *software* (art. 22).

Al fine di garantire un elevato livello di sicurezza informatica e la fiducia di tutte le parti interessate, particolare enfasi è posta al Capitolo IV sul raccordo con gli organismi di valutazione della conformità (cc.dd. organismi notificati) e, più a monte, con le autorità nazionali di notifica. In quest'ottica, gli Stati membri designano un'autorità responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione e la notifica degli organismi di valutazione della conformità, nonché per il monitoraggio degli stessi, in linea con la decisione 768/2008/CE e secondo i requisiti fissati nella proposta (art. 27). Gli organismi autorizzati e costituiti secondo il dettato dell'art. 29 eseguono le valutazioni di conformità secondo le procedure di cui all'art. 24 e all'All. VI in modo proporzionato e rigoroso. Ove abbiano ragione di ritenere che le prescrizioni di cui all'All. I o alle corrispondenti norme armonizzate o alle specifiche comuni *ex* art. 19 non siano state rispettate dal produttore, detti organismi negano il rilascio del certificato di conformità e sollecitano l'adozione delle pertinenti misure correttive. Se le criticità emergono durante il monitoraggio successivo al rilascio di un certificato, alla richiesta *de qua* può seguire la sospensione o il ritiro del certificato. Tali ultime ipotesi, assieme alla limitazione, costituiscono via obbligata in caso di mancata assunzione delle misure correttive o di fallimento delle stesse.

Altro modulo fondamentale del progetto riguarda la sorveglianza del mercato e l'*enforcement*, di cui al Capitolo V (v. Considerando 54). Al fine di garantire l'effettività delle misure in analisi, ciascuno Stato membro designa una o più autorità di vigilanza del mercato, con cui gli operatori economici sono tenuti a collaborare proficuamente. Inoltre, ai prodotti con elementi digitali rientranti nell'ambito di applicazione della proposta si applica il Reg. 2019/1020/UE (sulla vigilanza del mercato e sulla conformità dei prodotti) (v. Considerando 55). Particolari cautele sono riservate ai prodotti con elementi digitali che presentano un rischio significativo di cybersicurezza (artt. 45 e 46).

Da ultimo, deve farsi cenno al Capitolo VII, segnalando il dovere generale di riservatezza sulle informazioni e sui dati ottenuti dai soggetti interessati nello svolgimento dei loro compiti e delle loro attività (art. 52) e la disciplina delle sanzioni *ex* art. 53. Su quest'ultimo aspetto, la proposta fissa soglie massime e affida la concreta ponderazione alla discrezionalità dei legislazioni nazionali (v. Considerando 62): l'inosservanza dei requisiti essenziali di cui all'All. I e degli obblighi di cui agli artt. 10 e 11 è soggetta a sanzioni amministrative pecuniarie fino a 15 milioni di euro o, se il trasgressore è un'impresa, fino al 2,5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore; la violazione di qualsiasi altro obbligo conduce a sanzioni amministrative pecuniarie fino a 10.000.000 di euro o, se il trasgressore è un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Può concludersi riportando l'indicazione di cui al Considerando 68, che fa trasparire un indirizzo regolatorio flessibile, quasi reso *rebus sic stantibus*, per cui la Commissione dovrebbe riesaminare periodicamente la disciplina in analisi, in consultazione con le parti interessate, valutando la necessità di modifiche alla luce dell'evoluzione delle condizioni sociali, politiche, tecnologiche o di mercato.

VALENTINO RAVAGNANI

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

5. Verso il regolamento europeo di progettazione eco-sostenibile dei dispositivi mobili tecnologici.

Lo scorso 28 settembre 2022 si è conclusa la fase (c.d. *draft act*) dedicata all'invio di commenti in merito alla proposta di Regolamento europeo in materia di progettazione eco-sostenibile dei dispositivi mobili tecnologici («*laying down ecodesign requirements for mobile phones, cordless phones and slate tablets pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending*») (nel prosieguo, anche "Proposta di Regolamento" o "Proposta"). L'iniziativa euro-unitaria si inserisce nel più ampio *Piano d'azione per l'economia circolare*, presentato nel 2020 (*Circular Economy Action Plan - For a cleaner and more competitive Europe*) nonché con gli obiettivi del *Green Deal* europeo in materia di uso efficiente delle risorse.

Con questa proposta, la Commissione europea intende stabilire, in particolare, nuove norme in materia di progettazione e di produzione eco-compatibile e sostenibile dei dispositivi mobili, quali cellulari, telefoni e tablet. La proposta di regolamento rappresenta un altro passo di un lungo percorso avviato, prima, con l'istituzione del *Piano di lavoro sulla progettazione ecocompatibile* (2016-2019) e, poi, con la pubblicazione di un uno studio preparatorio in tema di progettazione ecocompatibile dei telefoni, smartphone e tablet, che già auspicava l'introduzione di norme specifiche per l'*ecodesign* e l'etichettatura energetica di questi prodotti tecnologici. Le regole contenute nella proposta di regolamento mirano a garantire una superiore efficienza energetica dei dispositivi prodotti e soprattutto una maggiore durata, una più facile riparabilità, una modificabilità in caso di errori o malfunzionamenti ed anche delle più elevate possibilità di riutilizzo o di riciclo. Così facendo, la proposta intende concorrere a un miglioramento delle prestazioni ambientali dei dispositivi tecnologici in termini di consumo di energia e di acqua, di livelli di emissione di CO2 e di efficienza dei materiali impiegati nella produzione, nonché favorire il riutilizzo e lo smaltimento dei prodotti nell'ottica di una economia ecosostenibile e circolare.

La proposta va ad ampliare la linea tracciata precedentemente dalla Direttiva 2009/125/CE relativa all'istituzione di un quadro europeo per l'elaborazione di regole specifiche per la progettazione sostenibile dei prodotti, da un lato, impedendo a dispositivi poco efficienti da un punto di vista energetico di essere immessi sul mercato e, dall'altro, concedendo ai consumatori la possibilità di compiere scelte maggiormente consapevoli. Per realizzare i suddetti obiettivi, si mira a costituire una cornice regolatoria orientata alla sostenibilità ambientale ed energetica dei prodotti e dispositivi tecnologici immessi sul mercato e che guarda all'intero ciclo del prodotto, dalla progettazione all'immissione nel mercato con le successive fasi di riparazione o riciclo.

La Proposta di Regolamento comprende una bozza di regolamento e sei allegati di supporto e si sviluppa secondo tre chiare linee direttive:

a) immettere sul mercato dispostivi duraturi ed efficienti dal punto di vista energetico;

b) assicurare ai consumatori un facile accesso alla riparazione, all'aggiornamento e alla manutenzione dei dispositivi mobili;

c) semplificare i processi di riuso e riciclo dei prodotti.

Gli **artt. 1-2** della Proposta specificano l'ambito applicativo del regolamento e le definizioni rilevanti a tal fine, escludendo alcune tipologie di dispositivi mobili *(«(a) mobile phones and tablets with a flexible main display which the user can unroll and roll up partly or fully; (b) smartphones designed for high security communication»)*. L'**art. 2**, specificatamente, fornisce le definizioni tecniche di *mobile phones*, *cordless phones* e *slate tablets*, che devono presentare determinati standard qualitativi ai fini della bozza di Regolamento. Le tre categorie di dispositivi, a cui si applica la Proposta, sono accumunate dal fatto di essere tutti dispositivi mobili con modalità di telecomunicazione a distanza ed informatica. L'**Allegato I** delimita il perimetro applicativo della proposta, attraverso l'elencazione di diversi dispositivi tecnologici impiegabili, le cui definizioni forniscono un quadro chiaro di applicazione della Proposta.

L'**art. 3**, invece, rimanda in merito agli standard tecnici e di eco-design da seguire all'**Allegato II** che contiene le diverse regole specifiche per i singoli dispositivi tecnologici impiegati.

In particolare, come si evince dall'**Allegato II («***Ecodesign requirements***»)**, la Commissione impone limiti (minimi) di durata – per contrastare anche il fenomeno della c.d. obsolescenza programmat*a* – sia per quanto riguarda l'uso dei dispositivi sia per quanto concerne la fase di manutenzione e riparazione. Il prodotto, infatti, deve garantire al consumatore un uso minimo di cinque anni dalla sua immissione nel mercato e deve essere assicurato l'accesso ai manuali di manutenzione per i sette anni successivi alla prima cessione del prodotto.

Nello specifico, così come esplicitato negli allegati tecnici, per facilitare il riciclo, si dovranno mettere pubblicamente a disposizione del singolo consumatore (per 15 anni a seguito dell'immissione sul mercato del prodotto) le istruzioni di manutenzione e accesso al software, con specifici passaggi tecnico-informatici da seguire. La proposta, inoltre, si concentra particolarmente sulla fase di riparazione del prodotto, entrando nel merito delle modalità di riparazione e imponendo standard qualitativi ai materiali utilizzati. In aggiunta a ciò, si mira a facilitare il procedimento per richiedere la riparazione del dispositivo, attraverso l'istituzione di procedure semplificate online.

L'**art. 4**, in merito alla valutazione di conformità, richiama l'art. 8 della Direttiva 2009/125/EC con l'obiettivo di rendere uniformi i processi valutativi dei prodotti tecnologici presenti nel mercato.

Ai fini delle procedure di controllo sul mercato («*Verification procedure for market surveillance purposes*»), l'**art. 5** fa da ponte tra le indicazioni contenute all'interno dell'**Allegato IV** e quanto disposto dall'art. 3 (2) della Direttiva 2009/125/EC (che prevede l'intervento dell'Autorità nazionali responsabili della sorveglianza sul mercato).

Inoltre, come mette in evidenza l'**art. 6** della bozza di regolamento, le nuove regole imporranno ulteriori standard e caratteristiche tecniche («*measures against circumvention*») ai dispositivi tecnologici immessi sul mercato, per garantire le già menzionate esigenze di sostenibilità energetica e di design eco-compatibile.

L'**art. 7**, invece, stabilisce che i riferimenti ai c.d. *indicative benchmarks* sono contenuti all'interno dell'**Allegato V**. Difatti, essi dovranno essere idonei a resistere ad urti, graffi od altro tipo di impatti, nonché ad acqua e polvere, oltre a dover rispettare specifici requisiti minimi in relazione alle batterie impiegate.

Infine, la disposizione dell'**art. 8** prevede un aggiornamento («*review*») della proposta alla luce dell'evoluzione tecnologica del mercato, da sottoporre al c.d. *Consultation Forum* istituito in virtù dell'art. 14 del Regolamento (UE) 2017/1369.

In conclusione, si è vicini all'approvazione di una importante iniziativa in ambito europeo che consolida la posizione (d'avanguardia) dell'Unione a favore della costituzione di un mercato unico sempre più sostenibile ed orientato al rispetto dell'ambiente, di standard energetici minimi – ad oggi, questione centrale a livello nazionale ed internazionale – e di obblighi informativi coerenti che diano la possibilità di scelte consapevoli ed informate ai consumatori.

ENZO MARIA INCUTTI

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12797-Progettazione-sostenibile-di-telefoni-cellulari-e-tablet-progettazione-ecocompatibile_it

6. Gli ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection.

L'8 settembre 2022 l'*European Law Institute* (c.d. ELI) ha emanato il *draft* dei *Principles on Blockchain Technology*, Smart Contracts and Consumer Protection (di seguito anche i "**Principi**" o il "**Framework**") la cui gestazione era iniziata sin dal 2018.

La Distribuited Ledgers Technology (c.d. "DLT"), nonché la blockchain e gli smart contracts che sono basati su di essa, sono fenomeni che evolvono rapidamente complicando e ritardando l'elaborazione di principi, e soprattutto di norme, organici in materia. Nondimeno, tale evoluzione solleva numerosi interrogativi a cui è difficile dare risposta anche in virtù dell'assenza di un framework giudico di riferimento sebbene, recentemente, l'Unione Europea abbia emanato diverse proposte legislative. Ci si riferisce al **Data Governance Act** (su cui v. notizia n. 4 nel numero 4/2021 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf e notizia n. 1 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf), al **Digital Finance Package** (su cui v. notizia n. 2 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf), all'**Artificial Intelligence Act** (su cui v. notizia n. 1 nel numero 2/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf), al **Digital Services Act** (su cui v. notizia n. 3 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf), al **Digital Market Act** e al **Data Act** (su cui v. notizie nn. 2 e 4 nel numero 1/2022 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf). Gli studi giuridici sulla blockchain e sugli smart contracts, peraltro, non sono ancora del tutto maturi, complice anche la continua evoluzione del fenomeno. I Reporters, dunque, hanno tentato di sviluppare quel framework giuridico sinora mancante, nell'ottica di fornire soluzioni armonizzate almeno tra gli Stati membri dell'UE, concentrandosi sull'elaborazione di un ristretto numero di principi e focalizzandosi, in particolare, sulla tutela dei consumatori. Il Framework è diviso in due parti: la prima dedicata ai principi di carattere generale; la seconda alla tutela dei consumatori coinvolti in smart contracts. Ogni Principio, a sua volta, si articola una black letter rule e in note esplicative.

Il Framework segue un approccio basato sulla neutralità tecnologica e sull'equivalenza funzionale. Per neutralità tecnologica si intende una soluzione applicabile a diversi tipi di rapporti giuridici a prescindere dal tipo di tecnologia utilizzata. Per equivalenza funzionale ci si riferisce al fenomeno per cui un accordo vincolante concluso offline debba avere lo stesso valore giuridico di uno

concluso sulla blockchain. Il Framework, inoltre, propone soluzioni giuridiche basate sul funzionamento in concreto della tecnologia blockchain (c.d. "Use-Case Approach").

Riguardo alla **Parte I**, va detto che il **Principio 1** a) identifica l'ambito di applicazione territoriale del Framework individuandolo sia negli Stati membri dell'UE sia in quelli extra UE. Il Principio 1 let. c), inoltre, chiarisce che il Framework detta norme valide solo per le transazioni realizzate tramite la blockchain e gli smart contracts (di seguito le "**Transazioni**") e non per il funzionamento di tali tecnologie. I Principi, inoltre, si concentrano su tematiche di civil law e, in particolare, sulle transazioni commerciali. Sono esclusi dal loro ambito di applicazione la creazione di diritti reali, la proprietà, il risarcimento, questioni successorie, matrimoniali e di convivenza.

Sempre al Principio 1, la let. b) chiarisce che il Framework intende stabilire una concezione comune di blockchain e smart contract, guidare i professionisti nell'applicazione delle norme esistenti in materia, stimolare ulteriori sviluppi sull'argomento e informare il pubblico delle best practices di settore. Ovviamente, tali obiettivi impongono un coordinamento con le normative eventualmente esistenti in materia.

Il **Principio 2** let. a) distingue le tipologie di smart contracts in: 1) meri codici privi di valore giuridicamente vincolante; 2) strumenti per eseguire accordi raggiunti al di fuori di una blockchain (c.d. Off-Chain); 3) contratti vincolanti; 4) una fusione tra smart contract stesso e accordo Off-Chain, che impone di stabilire se il contratto sia stato concluso sulla blockchain (c.d. On-Chain) o Off-Chain.

La già menzionata classificazione degli smart contracts discende dai diversi tipi di blockchain esistenti. Quest'ultima, infatti, può essere pubblica o privata a seconda che tutti o solo alcune persone possano parteciparvi. Nondimeno, è possibile distinguere tra blockchain c.d. "permissioned" o "permissionless" a seconda che solo le persone specificamente autorizzate o meno possano eseguire transazioni. I partecipanti alla rete, inoltre, possono essere privati, imprese o enti pubblici.

Al netto di questioni classificatorie, però, occorre chiedersi se gli smart contracts possano costituire accordi giuridicamente vincolanti. La risposta al quesito presuppone un'indagine caso per caso attenta alla natura delle parti coinvolte e alla tipologia di smart contract utilizzata, come afferma anche il **Principio 3**.

Ad ogni modo, gli smart contracts ben possono dare vita a contratti vincolanti e, in caso di disaccordo tra contratto concluso On-Chain (ossia concluso sulla blockchain) e Off-Chain, il Principio 2 let. a) 4) stabilisce che prevalga quest'ultimo.

Il **Principio 4** let a) stabilisce che alle transazioni realizzate sulla blockchain si applicano le stesse norme applicabili a quelle concluse Off-Chain, incluse quelle di diritto internazionale privato. Di conseguenza, è ammissibile pure la scelta di legge e del Foro competente (let. b) del Principio in commento). Il semplice fatto che la transazione avvenga tra i nodi di una rete che per definizione è decentralizzata, tuttavia, non costituisce un presupposto sufficiente ad applicare il diritto internazionale privato essendo comunque necessario un elemento di transnazionalità, il c.d. criterio di collegamento (let. c) del Principio in commento).

Il **Principio 5** è dedicato alla natura giuridica delle transazioni concluse sulla blockchain. Per affrontare il tema, i Reporters si sono basati sul Draft Common Frame of Reference (c.d. DCFR) che impone di effettuare una valutazione caso per caso considerando sia i soggetti della Transazione, che possono essere B2C, B2B o B2G, sia l'oggetto della medesima.

Il Principio afferma che una Transazione ben può costituire un'offerta, l'accettazione di un'offerta o altra dichiarazione con valore vincolante, così originandosi un accordo giuridicamente vincolante, laddove vi sia una manifestazione di volontà chiaramente riferibile ad una parte della Transazione.

Al riguardo, come fatto dal Framework, è utile rappresentare la posizione assai netta in favore della natura contrattuale delle transazioni concluse sulla blockchain della Court of Appeal di Singapore nel caso Quoine Pte Ltd v B2C2 Ltd, [2020] SGCA(I) 02. La sentenza, infatti, afferma: "*there is no reason why the normal rules should not apply just because a potential contract is a smart contract*". Analogamente, il Report "Smart Legal Contracts" della English Law Commission datato novembre 2021, sostanzialmente facendo proprie le conclusioni della UK Jurisdiction Taskforce, dichiara: "*smart legal contracts can satisfy the requirements for a contract*".

Il **Principio 6** prevede che le Transazioni siano efficaci a partire dal giorno stabilito dalle parti. Se queste non dispongono nulla, le transazioni On-Chain sono efficaci da quando il destinatario della proposta contrattuale viene a conoscenza di quest'ultima oppure la transazione è registrata sulla blockchain.

Il **Principio 7** è dedicato ai requisiti formali della Transazione e si basa sui concetti di equivalenza funzionale e neutralità tecnologica.

Innanzitutto, il Principio 7 let. a) stabilisce che laddove un ordinamento imponga dei requisiti di forma per un accordo, che siano replicati anche online, si deve ritenere che tali requisiti siano stati rispettati. Le successive lett. b) e c) del Principio in esame richiamano la nota distinzione tra "text form", ossia atto scritto, e "written form", ossia atto scritto e firmato, nata nel codice civile tedesco, il BGB.

Ora, la forma scritta è agevolmente replicabile sulla blockchain o negli smart contracts. Maggiori difficoltà, invece, presenta l'apposizione di una firma o il rispetto di una forma solenne. Eppure, il Principio 7 let. c) stabilisce che anche questi requisiti possono essere soddisfatti, qualora una Transazione: i) garantisca le stesse tutele previste per un contratto Off-Chain; ii) raggiunga l'obiettivo per cui sono stati imposti i requisiti formali e iii) soddisfi i dettami del Regolamento eIDAS.

Il **Principio 8** stabilisce che le parti possono scegliere la lingua di una Transazione.

In caso di contrasto tra la versione On-Chain e Off-Chain di un accordo, però, sorge una questione interpretativa sul linguaggio, naturale o informatico. In tal caso, il Framework non interviene dettando dei criteri interpretativi limitandosi a stabilire che sia la versione Off-Chain a prevalere (**Principio 9**).

Il Framework si occupa anche della risoluzione delle Transazioni stabilendo, al **Principio 10**, che laddove la legge applicabile preveda un diritto di risoluzione e questa sia esercitato da un contraente, esso si traduca in una transazione inversa rispetto a quella che si desidera risolvere (c.d. reverse transaction).

Eventuali controversie tra le parti di una Transazione possono essere rimesse ad un arbitrato (**Principio 11**). Sebbene tale soluzione sia stata sostenuta anche nel Report sul "Digital Dispute Resolution Rules" della UK Jurisdictional Taskforce, permangono alcuni interrogativi al riguardo, soprattutto laddove la normativa applicabile alla Transazione richieda la "classica" forma scritta della clausola compromissoria.

Il **Principio 12** prevede che le parti deboli di una Transazione debbano godere della medesima tutela di cui beneficerebbero in caso di accordo Off-Chain. Una transazione On-Chain, infatti, non può essere il mezzo per ridurre le tutele dei consumatori.

La **Parte II** del Framework detta una serie di principi proprio a tutela dei consumatori.

Come noto, l'art. 2 dir. 2019/771/UE definisce questi ultimi come "*qualsiasi persona fisica che … agisca per fini che non rientrano nel quadro dell'attività commerciale, industriale, artigianale o professionale di tale persona*". E' ben possibile, tuttavia, che le imprese, soprattutto quelle medio piccole, si trovino in una situazione equiparabile a quella dei consumatori, ovvero di debolezza, nei propri rapporti commerciali. Di conseguenza, sebbene i Reporters affermino che il Framework è stato volutamente elaborato concentrandosi sul consumatore persona fisica, nulla vieta che esso possa applicarsi anche nei rapporti tra pari (c.d. Peer to Peer), ossia tra imprese.

Ciò detto, il **Principio 13** let. a) afferma chiaramente che la tutela dei consumatori non può essere pregiudicata dal fatto che una transazione avviene sulla blockchain. Facendo buon uso dei criteri di neutralità tecnologica ed equivalenza funzionale, il Principio 13 let. b) afferma che i consumatori hanno diritto alla medesima protezione per le transazioni concluse Off-Chain e On-Chain; "*l'uso della tecnologia BLOCKCHAIN o di uno SMART CONTRACT non dovrebbe privare i consumatori di alcun diritto"* (let. c)). Di conseguenza, le imprese che ricorrano agli smart contracts sono tenute ad assicurasi che i consumatori possano esercitare i propri diritti come se si trattasse di una transazione Off-Chain. La circostanza per cui un rimedio giuridico sia troppo difficile da implementare sulla blockchain, infatti, non può consentire eccezioni alla tutela dei consumatori. Tale impostazione dei Principi tiene conto del fatto che le transazioni online sono spesso meno trasparenti e controllabili rispetto a quelle Off-Chain.

Sempre per tale motivo, il Principio 13 let. f) prevede che i consumatori, i quali in buona fede abbiano concluso una Transazione devono essere tutelati da eventuali pattuizioni Off-Chain, tra l'impresa che abbia stipulato la Transazione col consumatore e soggetti terzi, le quali pregiudichino i diritti della parte debole.

Il **Principio 14** ammette che nei contratti coi consumatori le parti possano scegliere la legge regolatrice dell'accordo e il Foro competente a risolvere eventuali controversie nascenti da esso senza, però, ledere i diritti dei consumatori.

Il **Principio 15** stabilisce, per quanto ci interessa, che i consumatori abbiano diritto a ricevere una copia scritta - nel linguaggio naturale - degli smart contracts, che, come noto, consistono in un codice informatico. La ratio di tale previsione è evitare che le Transazioni ledano gli interessi dei consumatori. Per questo motivo, i Reporters propongono anche due soluzioni per verificare che lo smart contract pregiudichi gli interessi dei soggetti deboli. La prima consiste nella conduzione di un audit sullo smart contract per assicurarsi che esso non leda i diritti fondamentali dei consumatori. La seconda soluzione, ispirato dall'art. 5 dir. 1993/13/CE s.m.i., impone che i termini contrattuali

siano sempre redatti per iscritto in forma intellegibile; in caso di dubbio sul significato di una pattuizione, però, prevale sempre l'interpretazione più favorevole al consumatore.

Il **Principio 16**, ispirato dai criteri di neutralità tecnologica ed equivalenza funzionale, rappresenta l'evoluzione dei precedenti Principi 8 e 13, laddove alle lett. a) e b) afferma che i consumatori, i quali concludano una Transazione hanno diritto alle stesse informazioni pre-contrattuali e post-contrattuali che avrebbero avuto se avessero concluso un classico contratto Off-Chain. Le successive lett. c) e d) del Principio, ricordano che tali informazioni debbano sempre essere disponibili per iscritto in linguaggio naturale. Nondimeno, al consumatore spetta un documento esplicativo delle previsioni dello smart contract. Laddove lo smart contract differisca dal suddetto documento, quest'ultimo prevarrà sul testo contrattuale.

Il **Principio 17** è dedicato al diritto di ripensamento e recesso.

Il consumatore ha diritto di essere informato dell'esistenza in suo favore di un periodo di ripensamento (c.d. "cooling-off period"), il quale ovviamente deve essere codificato nello smart contract, e che egli potrà esercitare ogni diritto connesso al menzionato periodo con una transazione tanto On-Chain, quanto Off-Chain. Per far si che tale periodo di ripensamento sia effettivo, la let. b) del Principio in commento stabilisce che lo smart contract potrà produrre effetti solo dopo che sia decorso tale arco temporale senza che il consumatore abbia esercitato il diritto di recesso.

Quest'ultimo deve consistere in una transazione inversa che sostanzialmente annulla la precedente con cui il contratto era stato concluso (let. d) del Principio). Il consumatore deve altresì essere informato di eventuali diritti (e obblighi) connessi all'esercizio del recesso, qualora previsti dalla normativa applicabile, e che la transazione inversa abbia avuto luogo.

Il **Principio 18**, infine, è dedicato alle clausole vessatorie e stabilisce che i consumatori debbano godere di una tutela effettiva per le transazioni concluse sia On-Chain sia Off-Chain (let. a) del Principio 18). Di conseguenza, essi devono poter risolvere On-Chain (oltreché Off-Chain) un contratto concluso online. Altrimenti la protezione riconosciutagli sarebbe compromessa.

Il Principio in commento alla let. b), inoltre, precisa che la previsione per cui un contratto può essere concluso solo online non è di per sé vessatoria.

Assai utilmente, poi, la let. d) del Principio 18 stabilisce che la dir. 1993/13/CE s.m.i. e l'acquis communautaire formatosi riguardo alla suddetta direttiva si applicano alle clausole vessatorie degli smart contracts. In presenza di clausole vessatorie self executing, inoltre, il consumatore ha diritto alla ricodifica dello smart contract per eliminare la clausola in commento.

La let. e) del Principio 18, infine, stabilisce che laddove una clausola sia stata dichiarata vessatoria in una class action, allora il professionista deve eliminarla da tutti gli smart contracts che la prevedano.

EMANUELE STABILE

https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection_Council_Draft.pdf

7. Il parere congiunto EDPB-EDPS sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori.

Il 28 luglio 2022 l'European Data Protection Board ("EDPB", ex WP 29) e l'European Data Protection Supervisor ("EDPS") hanno pubblicato, ai sensi dell'art. 42, paragrafo 2, del Regolamento UE n. 2018/1725, il parere congiunto n. 4/2022 (il "parere") sulla proposta di regolamento della Commissione europea del 11.5.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori ("proposta di regolamento).

La proposta di regolamento è destinata a sostituire il regolamento (UE) 2021/1232, entrato in vigore nel 2021 come misura temporanea per consentire ad alcune categorie di fornitori di servizi di individuare e segnalare abusi sessuali su minori online e di rimuovere dai loro servizi materiale pedopornografico, nel rispetto della normativa europea sulla protezione dei dati personali.

Tale proposta di regolamento impone obblighi qualificati ai fornitori di servizi di hosting, di servizi di comunicazione interpersonale e di altri servizi, in merito alla individuazione, la segnalazione, la rimozione e il blocco di materiale online noto e nuovo relativo ad abusi sessuali su minori ("CSAM"), nonché l'adescamento di minori. Tali fornitori saranno obbligati a valutare e mitigare il rischio di abuso sui loro servizi e qualsiasi misura adottata dovrà essere proporzionata e soggetta ad adeguate garanzie. Il regolamento proposto istituirà anche un Centro Europeo sugli abusi sessuali sui

minori e delle autorità nazionali di coordinamento, che faciliteranno l'attuazione del regolamento proposto.

Nel parere, l'EDPB e l'EDPS condividono il loro punto di vista sulla questione di come trovare il giusto equilibrio tra il diritto alla riservatezza delle comunicazioni e della vita privata e familiare, il diritto alla protezione dei dati personali (artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea) e gli sforzi per affrontare l'abuso sessuale dei minori online.

I due enti sollevano una serie di preoccupazioni in merito alla proposta di regolamento, in particolare per quanto riguarda la questione se le interferenze con i diritti fondamentali che prevede siano "necessarie" e "proporzionate" e come tali termini debbano essere interpretati in questo contesto. Nel fare ciò, vengono richiamate decisioni della CGUE relative a misure legislative che violano i diritti fondamentali in settori quali la giustizia penale e la sicurezza nazionale, tra cui i casi *Digital Rights Ireland*, *Tele2Sverige* e *Watson*, *Schrems* e *La Quadrature du Net.* La proposta di regolamento della Commissione potrebbe presentare più rischi per gli individui e per la società in generale che per i criminali perseguiti da CSAM; il rischio è che la proposta di regolamento possa diventare la base per una scansione generalizzata e indiscriminata dei contenuti di praticamente tutti i tipi di comunicazioni elettroniche.

Tanto premesso, l'EDPB e l'EDPS hanno espresso, al riguardo, una serie di raccomandazioni e osservazioni, di seguito sintetizzate:

La proposta di regolamento abrogherebbe il regolamento 2021/1232 ed eliminerebbe l'attuale regime in base al quale è consentito il trattamento dei dati personali al fine di individuare e rimuovere gli abusi sessuali su minori online su base volontaria, sostituendolo con un regime obbligatorio. L'EDPB e l'EDPS raccomandano di chiarire che, in tali circostanze, i fornitori di servizi che non saranno obbligati a effettuare tali trattamenti ai sensi della proposta di regolamento non potranno più procedere su base volontaria, a meno che ciò non sia previsto dalle leggi nazionali ad essi applicabili che recepiscono la Direttiva 2002/58/CE (Direttiva ePrivacy).

L'EDPB e l'EDPS ritengono che le disposizioni della proposta di regolamento relative alle valutazioni dei rischi che i fornitori di servizi devono effettuare non siano sufficientemente dettagliate e precise per soddisfare i requisiti di certezza, chiarezza e prevedibilità necessari qualora si vada a interferire con il godimento dei diritti fondamentali. La criticità riguarderebbe, in particolare, le disposizioni che regolano la procedura per l'emissione di ordini di individuazione, mirata a un fornitore di servizi. Le tecnologie per l'individuazione di CSAM nuove o sconosciute, rispetto a quelle note, hanno tassi di errore significativamente più elevati e il loro utilizzo potrebbe quindi avere un impatto sproporzionato sui diritti fondamentali (a causa dei falsi positivi).

Viene inoltre rilevato che il regime che si applicherà agli ordini di rilevamento potrebbe indurre i fornitori di servizi soggetti alla proposta di regolamento, a smettere di utilizzare la crittografia end-to-end o a ridurre in altro modo l'efficacia dei loro accordi di crittografia; ciò sarebbe dovuto alla possibilità di dover, da parte di un fornitore dei servizi di specie, ottemperare, in un breve lasso di tempo, ad un ordine di rilevamento da parte di una autorità giudiziaria/amministrativa competente, pena l'applicazione di una sanzione. Su questa base, i due enti si oppongono all'inclusione nella proposta di regolamento di qualsiasi misura che possa, anche indirettamente, indebolire le pratiche di crittografia.

L'EDPB e l'EDPS, peraltro, sono particolarmente critici nei confronti della disciplina della proposta di regolamento che prevede la scansione delle comunicazioni audio al fine di individuare l'adescamento di minori (cosa non consentita dal regolamento 2021/1232). Nel parere osservano che ciò richiederebbe un'intercettazione continua e in diretta, particolarmente invasiva. Hanno inoltre espresso scetticismo nei confronti dell'uso proposto di misure di verifica dell'età per identificare gli utenti minorenni dei servizi, in quanto riconoscono che attualmente non esiste una soluzione tecnologica in grado di valutare l'età con certezza, con il risultato che il fornitore di servizi potrebbe essere incentivato a escludere dall'accesso ai servizi gli adulti dall'aspetto giovanile, oppure a impiegare misure di verifica eccessivamente molto intrusive.

In conclusione, l'EDPB e l'EDPS evidenziano come la proposta di regolamento sollevi serie preoccupazioni in materia di protezione dei dati personali e invitano il legislatore dell'UE a modificarlo per colmare le lacune individuate nel parere, in particolare per quanto riguarda il rispetto dei criteri di necessità e proporzionalità. Nell'attesa che venga adottato il nuovo provvedimento, anche alla luce delle modifiche proposte dall'EDPB e dall'EDPS, i fornitori i cui servizi possono essere utilizzati per condividere abusi sessuali su minori online o per adescare minori online, potranno continuare a cercare di affrontare tali attività su base volontaria ai sensi del regolamento 2021/1232.

FRANCESCO GROSSI

https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

8. NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti.

Il 24 agosto 2022 l'organizzazione non governativa NOYB – *European Center for Digital Rights* (NOYB) ha presentato davanti all'Autorità francese per la protezione dei dati (*Commission nationale de l'informatique et des libertés*, nel prosieguo "**CNIL**") una denuncia contro Google per l'invio di e-mail pubblicitarie non richieste – senza un valido consenso degli utenti – attraverso la piattaforma di posta elettronica Gmail.

Google, infatti, invia agli utenti Gmail messaggi pubblicitari che compaiono direttamente nella loro casella di posta come normali e-mail. Trattandosi di comunicazioni aventi contenuto promozionale, queste rientrano nella categoria del marketing diretto e, come tali, sono soggette all'applicazione della Direttiva 2002/58/CE ("**Direttiva ePrivacy**"), secondo cui l'invio di materiale pubblicitario o di comunicazioni commerciali è consentito solo previo un valido consenso espresso dell'utente destinatario. Tuttavia, mentre per i messaggi di posta indesiderata (c.d. *spam*) esterni Gmail opera automaticamente un filtro spostando le e-mail direttamente in una cartella separata, i messaggi promozionali non richiesti di Google vengono inviati direttamente alla casella di posta dell'utente senza che sia applicato alcun filtro.

Sul tema si era pronunciata anche la Corte di Giustizia dell'Unione Europea con la sentenza del 25 novembre 2021, StWL Städtische Werke Lauf a.d Pegnitz (C-102/20) in cui affermava che la visualizzazione nella casella e-mail in arrivo di messaggi pubblicitari in una forma simile a quella di un vero e proprio messaggio di posta elettronica (c.d. *inbox* advertising) costituisce un uso della posta elettronica a fini di commercializzazione diretta ai sensi della Direttiva ePrivacy. Secondo quella sentenza, tali messaggi presentano un elevato rischio di confusione per l'utente che può essere indotto a cliccare sulla stringa corrispondente al messaggio pubblicitario ed essere così reindirizzato al sito Internet contenente la relativa pubblicità senza aver prestato alcun consenso. I messaggi di *inbox advertising*, infatti, si distinguono visivamente dall'elenco degli altri messaggi di posta elettronica solo per il fatto che la data è sostituita dalla dicitura "Annuncio" e non è menzionato alcun mittente.

Nonostante la citata pronuncia della Corte europea, Google ha continuato ad utilizzare lo strumento dell'*inbox advertising* senza il consenso degli utenti, violando così la normativa applicabile. Per questo motivo NOYB ha presentato la denuncia all'autorità francese che potrà decidere direttamente, senza dover consultare autorità di controllo di altri Paesi UE. Trattandosi infatti di una violazione della Direttiva ePrivacy e non del Regolamento UE 2016/619 ("**GDPR**") non opera il meccanismo di cooperazione previsto dall'art. 60 GDPR.

CHIARA RAUCCIO

https://noyb.eu/it/gmail-crea-email-di-spam-nonostante-la-sentenza-della-cgue

9. Il Garante privacy esprime parere negativo sullo schema di decreto sull'Ecosistema Dati Sanitari.

Il 22 agosto 2022 l'autorità Garante per la protezione dei dati personali ("**Garante privacy**" o "**Garante**") ha emesso un parere negativo sullo schema di decreto presentato dal Ministero della salute e dal Ministero per l'innovazione tecnologica e la transizione digitale che prevede la realizzazione del c.d. Ecosistema Dati Sanitari ("**EDS**"). L'istituzione dell'EDS, prevista dall'art. 12, comma 15-quater del d.l. n. 179/2012 con l'obiettivo di "garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale", si inserisce nell'ambito della riforma del Fascicolo sanitario elettronico ("**FSE**"). Per tale motivo il Garante si è pronunciato parallelamente – chiedendo alcune modifiche – anche sullo schema di decreto sul FSE che risulta preliminare a quello sull'EDS.

Il Garante privacy ha precisato di condividere l'esigenza di introdurre strumenti che agevolino lo sviluppo di servizi sanitari digitali; tuttavia, ha sottolineato come questo non possa avvenire a discapito dei diritti fondamentali dei cittadini, il cui rispetto deve sempre essere tenuto nella massima considerazione. Questo risulta particolarmente vero nel caso in esame in quanto lo schema di decreto prevede la costituzione di quella che il Garante ha definito la "più grande banca dati sulla salute del nostro Paese". L'EDS, infatti, comporterebbe la duplicazione di dati e documenti sanitari già

presenti nel FSE dando luogo a un database che raccoglierebbe a livello centralizzato, senza garanzie di anonimato per gli assistiti, dati e documenti sanitari relativi a tutte le prestazioni sanitarie erogate sul territorio nazionale. Considerata la quantità e la delicatezza dei dati trattati, nonché la presenza di un trattamento sistematico su larga scala anche attraverso logiche algoritmiche, si rende necessaria una regolamentazione che garantisca il pieno rispetto dei principi generali del Regolamento UE 2016/679 (“**GDPR”)**. Al contrario, il Garante ha ravvisato una serie di violazione della disciplina in materia di protezione dei dati personali che lo hanno portato ad esprimere un parere negativo sullo schema di decreto, indicando ai Ministeri competenti le misure necessarie per superare le criticità riscontrate.

In particolare, il Garante ha osservato come lo schema di decreto non adempia alla funzione ad esso assegnata dall’art. 12, comma 15-quater del d.l. 179/2012 – delineare “i contenuti dell’EDS, le modalità di alimentazione dell’EDS, nonché i soggetti che hanno accesso all’EDS, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati” – in quanto non disciplina specificamente tali aspetti, ma si limita a delineare un quadro generale rinviando la disciplina di dettaglio a una serie di successivi decreti non ancora emanati. In questo modo il decreto risulta una “scatola vuota” dal contenuto indeterminato che rende impossibile all’autorità una effettiva valutazione della correttezza e adeguatezza dei trattamenti, in particolare con riferimento ai principi di proporzionalità e minimizzazione dei dati.

Anche sui diritti degli interessati, lo schema di decreto rinvia sommariamente ai diritti esercitabili con riferimento al trattamento effettuato attraverso il FSE. Tuttavia, come sottolinea il Garante, i trattamenti effettuati mediante il FSE e quelli effettuati in relazione all’EDS presentano numerose differenze sotto il profilo delle finalità perseguite e della relativa titolarità. Pertanto, il rinvio non permette di chiarire alcuni temi quali le modalità e le conseguenze dell’esercizio del diritto di oscuramento e di revoca del consenso.

Ulteriori criticità sono date dall’estrema genericità nell’indicazione dei servizi resi dall’EDS, nonché dalla mancata previsione di livelli diversificati di accesso a tali servizi e dalla scarsa chiarezza sui ruoli privacy assunti dai diversi soggetti coinvolti nelle fasi di raccolta ed elaborazione dei dati.

Infine, il Garante ha riscontrato numerose imprecisioni e carenze (in particolare nell’individuazione dei rischi per gli interessati) nella valutazione d’impatto svolta ai sensi dell’art. 35 GDPR dal Ministero della salute e fornita all’autorità ancora in versione “bozza”. Anche in questo caso il Garante ha fornito indicazioni sulle necessarie modifiche e integrazioni del documento invitando il Ministero a coinvolgere nella valutazione del rischio anche strutture con competenze mediche ed etiche.

A seguito del parere in esame, lo schema di decreto torna nelle mani dei Ministeri competenti che dovranno quanto prima provvedere a riformularlo alla luce delle considerazioni del Garante al fine di ottenere il parere positivo dello stesso per procedere alla creazione dell’EDS.

CHIARA RAUCCIO

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9802752

10. Accesso ai risultati della ricerca scientifica finanziata con fondi federali: nuove linee guida negli Stati Uniti.

In data 25 agosto 2022, l’*Office of Science and Technology Policy* (OSTP) del governo federale degli Stati Uniti ha pubblicato le nuove linee guida per garantire un accesso equo, immediato e libero ai risultati della ricerca scientifica finanziata dal governo federale con fondi pubblici (“*Memorandum OSTP* 2022”). L’obiettivo dichiarato del governo americano è quello di garantire le stesse opportunità non solo di accesso ai risultati della ricerca, ma anche di partecipazione attiva di tutta la comunità americana al progresso scientifico del Paese, contrastando quelle che a tutt’oggi rappresentano forme di discriminazione all’accesso alla scienza e, più in generale, alla cultura.

In questa prospettiva, la Casa Bianca ha stabilito che tutte le ricerche finanziate dalle agenzie federali (ovvero l’equivalente dei nostri Ministeri) debbano essere pubblicate in modo tale che siano immediatamente e gratuitamente consultabili dal pubblico.

Un precedente intervento in questa direzione risale al 2013 (cd. *Memorandum OSTP 2013*) ed ha rappresentato un punto di svolta senza precedenti, giacché in grado di innescare movimenti sociali per il libero accesso alla ricerca che, di lì a poco, si sarebbero diffusi in tutti i singoli Stati americani ed anche oltre i confini degli stessi. Negli anni successivi, le stesse agenzie federali soggette al *Memorandum OSTP* 2013 hanno sviluppato piani e attuato politiche in coerenza con le indicazioni ricevute dal governo.

Nel *Memorandum OSTP* 2022 vengono fornite nuove linee guida alle agenzie per l'aggiornamento delle politiche di accesso aperto. In particolare, l'OSTP raccomanda di:

- aggiornare le proprie politiche di accesso pubblico non oltre il 31 dicembre 2025, al fine di rendere accessibili le pubblicazioni e i dati, eliminando l'attuale embargo di un anno, così da renderli gratuiti e accessibili a tutti;
- stabilire procedure che garantiscano la trasparenza e l'integrità della ricerca scientifica nelle politiche di accesso;
- coordinarsi con l'OSTP per garantire un'equa distribuzione dei risultati e dei dati della ricerca finanziati a livello federale.

Le principali novità introdotte con questo intervento sono dunque:

i) eliminazione dell'embargo di 12 mesi per gli articoli scientifici peer-reviewed finanziati dal governo federale: prima di questa previsione, l'accesso ai risultati della ricerca finanziata a livello federale era a pagamento o limitato solo a coloro che avevano accesso attraverso biblioteche o altre istituzioni; ora, mezzi finanziari e accesso privilegiato non devono più costituire un prerequisito per accedere ai benefici della ricerca finanziata dal governo federale e, quindi, dai contribuenti americani;

ii) rafforzamento dei piani di condivisione dei dati rispetto al Memorandum 2013, rendendoli immediatamente disponibili al momento della pubblicazione: fornire i dati a supporto di nuovi articoli scientifici migliora la trasparenza e la possibilità di basarsi sui risultati delle ricerche precedenti. L'accesso del pubblico ai dati di ricerca finanziati dal governo federale aiuta anche a "livellare" il terreno su cui misurarsi, in un panorama di finanziamenti altamente diseguale tra le diverse discipline e comunità accademiche, offrendo così la possibilità a studiosi, discenti e in più in generale al pubblico, un uso secondario dei dati, altrimenti indisponibili. Le nuove linee guida chiariscono, inoltre, che la condivisione dei dati deve avvenire in modo responsabile e alle stesse agenzie è richiesto di garantire la protezione del diritto alla *privacy* e alla sicurezza nella circolazione dei dati.

Tuttavia, garantire che tutti i cittadini americani possano beneficiare in modo equo e libero di questo importante mutamento nelle politiche di *open access* richiede tempo, impegno e collaborazione da parte di tutte le agenzie e dei soggetti a vario titolo coinvolti. In tal senso, l'*Office of Science and Technology Policy* ha annunciato il ricorso a diverse risorse per supportare questo cambiamento.

Attraverso una nuova sottocommissione del *National Science and Technology Council on Open Science* (SOS), l'OSTP sta conducendo un processo di coordinamento per garantire che le politiche di accesso pubblico siano accompagnate e sostenute in maniera graduale, soprattutto per le componenti più vulnerabili dell'ecosistema della ricerca, incapaci di sostenere i costi crescenti associati alla pubblicazione di articoli ad accesso aperto, come i ricercatori in fase iniziale o di istituzioni al servizio delle minoranze. Le nuove linee guida, inoltre, consentono ai ricercatori di includere nelle loro proposte di *budget* di finanziamento alla ricerca i costi di pubblicazione e condivisione dei dati.

Si sottolinea, altresì, la necessità di combattere le disuguaglianze esistenti nella distribuzione dei finanziamenti: molte agenzie federali, tra cui il Dipartimento dell'Energia, il *National Institutes of Health* e la *National Science Foundation*, hanno lanciato programmi volti a concedere sovvenzioni a sostegno della fase iniziale delle carriere dei ricercatori, azzerando ogni forma di discriminazione basata sulla razza e sul genere. L'OSTP ha anche pubblicato il report *Economic Landscape of Federal Public Access Policy* per aiutare a comprendere meglio i potenziali impatti economici di questi cambiamenti politici su tutta la popolazione.

LUCIO CASALINI

https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf

11. Le proposte normative dell'11 ottobre 2022 del Financial Stability Board in materia di cripto-attività e global stablecoins.

L'11 ottobre 2022 il *Financial Stability Board* ("**FSB**") ha avviato una consultazione sulla proposta per una regolamentazione internazionale delle cripto-attività. La proposta consta di due documenti principali: (i) raccomandazioni per un quadro regolamentare e di vigilanza dei servizi e mercati in cripto-attività (anche, "**raccomandazioni**"); (ii) revisione delle raccomandazioni per la regolamentazione e la vigilanza dei c.d. *global stablecoins* ("**GSCs**") *arrangements* (anche, "**revisione**"). La consultazione avrà termine a dicembre 2022.

Quanto alle raccomandazioni per un quadro regolamentare delle cripto-attività, a partire da un'analisi del mercato attuale e delle iniziative

regolamentari intraprese, il FSB riconosce come sia necessario promuovere degli approcci di regolamentazione e vigilanza che siano completi e tra loro coerenti, dati i rischi che ne potrebbero derivare per la stabilità finanziaria a livello globale. Ne segue che le raccomandazioni delineate dovrebbero applicarsi a tutte le cripto-attività e giurisdizioni.

In generale, le autorità dovrebbero disporre di adeguati poteri e strumenti per la regolamentazione e supervisione dei servizi e mercati in cripto-attività (*Recommendation* 1), nonché predisporre un quadro normativo che vada a disciplinare sia gli emittenti che i prestatori di servizi (*Recommendation* 2). In particolare, tale quadro normativo dovrebbe ispirarsi al principio "*same activity, same risk, same regulation*" e, quindi, guardare non alla forma, ma bensì alla funzione economica svolta dalla cripto-attività o dall'operatore di mercato considerato.

Il FSB sottolinea anche come le cripto-attività abbiano natura *cross-border* e come, dunque, ciascun approccio regolamentare e di supervisione dovrebbe prevedere cooperazione e coordinamento tra le diverse autorità, sia a livello domestico che internazionale (*Recommendation* 3).

Nel documento di consultazione si evidenzia poi come un eventuale quadro regolamentare dovrebbe affrontare specifici rischi e aspetti delle cripto-attività. In particolare, il focus ricade sulle attività di *risk management* e di *data management*, nonché sulla *governance* delle iniziative di cripto-attività. In particolare, secondo la proposta, gli emittenti e prestatori di servizi in cripto-attività dovrebbero predisporre una struttura di governo societario trasparente che identifichi chiaramente le responsabilità e i ruoli degli attori coinvolti (*Recommendation* 4), nonché un *framework* adeguato per la raccolta e gestione dei dati e per la *disclosure* di informazioni rilevanti (*Recommendation* 6 e *Recommendation* 7). In aggiunta, i prestatori di servizi in cripto-attività dovrebbero dotarsi di robusti sistemi di gestione del rischio, con particolare attenzione ai rischi per la stabilità finanziaria (*Recommendation* 5).

Da ultimo, si sottolinea come le autorità dovrebbero identificare e monitorare le interconnessioni - sia nello stesso ecosistema delle cripto-attività che con il sistema finanziario tradizionale-che potrebbero sfociare in rischi per la stabilità finanziaria (*Recommendation* 8) e contenere quei rischi che potrebbero derivare dall'esercizio congiunto di più funzioni e attività in capo a uno stesso soggetto (*Recommendation* 9). In particolare, quanto all'ultimo punto, il focus dovrebbe ricadere su quei prestatori di servizi in cripto-attività verticalmente integrati, quali, ad esempio, le piattaforme di scambio di cripto-attività.

Quanto alle raccomandazioni per la regolamentazione e supervisione dei GSCs, la proposta consiste in una revisione delle *High-Level Recommendations* già definite nel 2020. Sebbene l'obiettivo rimanga quello di promuovere approcci regolatori coerenti ed efficaci, ciò che cambia è l'ambito di applicazione. Nonostante la dimensione del mercato sia ancora contenuta e limitata all'ecosistema delle cripto-attività, il FSB riconosce come i GSCs potrebbero rapidamente crescere in rilevanza e diffusione. Sicché, nel delineare un quadro normativo, sarebbe necessario non solo considerare i GSCs, ma anche quegli *stablecoins* potenzialmente capaci di diventare GSCs in un futuro prossimo. In ogni caso, si sottolinea come tali *stablecoins* dovrebbero comunque essere sempre soggetti alle raccomandazioni definite per le cripto-attività in generale.

Dopodiché, nella revisione si enfatizza come le autorità dovrebbero essere pronte a contenere i rischi per la stabilità finanziaria che potrebbero derivare dai GSCs (*High-level Recommendation* 1) ed esercitare un controllo completo su quelle che sono le attività e funzioni dei GSCs (*High-level Recommendation* 2). Particolare attenzione dovrebbe essere posta dalle autorità ai *wallet service providers* e alle *trading platforms*, data la criticità di di tali servizi per la stabilizzazione del valore e custodia dei GSCs.

La revisione ha poi ad oggetto il rafforzamento di alcuni punti circa aspetti critici dei GSCs, quali, ad esempio, la struttura di governo societario o sistemi di gestione del rischio. In particolare, la revisione mira a rendere chiaro come la struttura di governo societario dei GSCs debba essere definita in modo trasparente e in maniera tale da non impedire l'applicabilità della regolamentazione e degli *standard* vigenti (*High-level Recommendation* 4). Nei sistemi di gestione del rischio, invece, particolare attenzione dovrebbe essere posta alle misure in materia di riciclaggio di denaro e finanziamento del terrorismo, nonché ad aspetti di *liquidity risk management* da attivare nel caso di fenomeni di *run* (*High-level Recommendation* 5).

In merito alla gestione e raccolta di dati, la revisione propone di dare potere all'Autorità di accedere ai dati rilevanti quando necessario per fini regolamentari, a prescindere da dove questi siano localizzati (*High-level Recommendation* 6).

Particolare attenzione viene poi riservata a quegli elementi che contribuiscono alla stabilizzazione del valore dei GSCs. In particolare, oltre a obblighi informativi generali, la revisione prevede la *disclosure* dei *reserve assets* e dei

dettagli del processo e dei diritti di rimborso degli utenti (High-level Recommendation 8). Ciò nella misura in cui l'emittente non sia già soggetto a requisiti informativi analoghi sotto altri *framework* regolamentari. Sempre in merito alla stabilizzazione del valore, la revisione si focalizza anche sulla redimibilità dei GSCs, prevedendo che tutti gli utenti debbano avere un chiaro diritto rimborso nei confronti dell'emittente o dei *reserve assets* (High-level Recommendation 9). In aggiunta, per assicurare la stabilizzazione del valore ed evitare fenomeni di panico, le autorità dovrebbero richiedere ai GSCs di dotarsi di meccanismi di stabilizzazione efficaci, procedure di rimborso chiare e rispettare i requisiti prudenziali di capitale e liquidità.

Da ultimo, la revisione prevede come i GSCs dovrebbero essere conformi a ogni requisito regolamentare, sia specifico che generale, applicabile già prima dell'avvio delle operazioni (*High-level Recommendation* 10).

ALICE FILIPPETTA

https://www.fsb.org/2022/10/regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-consultative-report/

https://www.fsb.org/2022/10/review-of-the-fsb-high-level-recommendations-of-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-consultative-report/