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. La Carta dei diritti digitali presentata dal Governo spagnolo il 14 luglio 2021.

Il 14 luglio 2021 il governo spagnolo ha presentato la *Carta derechos digitales* (**"*Carta*"**), un documento non normativo che afferma il valore della persona e della dignità umana nella definizione delle regole e delle politiche della nuova realtà digitale. Redatto da un gruppo di esperti di discipline diverse, la *Carta* è il risultato di circa un anno di lavori e di due consultazioni pubbliche. Il testo si compone di ventotto disposizioni suddivise in sei sezioni e anticipate da un preambolo che da conto delle ragioni dell'intervento, centrale nella c.d. *Plan España Digital 2025*.

La prima sezione della *Carta*, intitolata *Derechos de libertad*, si apre con il riferimento al rispetto negli ambienti digitali dei diritti fondamentali riconosciuti nelle diverse carte e dichiarazioni e prosegue con l'affermazione del diritto all'identità, alla protezione dei dati (con esplicito richiamo al Regolamento UE 2016/679, il GDPR) e al diritto all'utilizzo di uno pseudonimo. A tal proposito, la Carta prevede che tale pretesa possa essere limitata solo quando l'identificazione personale sia necessaria e che sia comunque possibile l'identificazione dell'utente ove richiesto dall'autorità giudiziaria. La medesima sezione prevede poi che il ricorso a sistemi di analisi che impieghino decisioni automatizzate o la profilazione degli individui sia possibile solo quando ammesso dalla normativa nonché il diritto di tutte le persone a strumenti di sicurezza adeguati a un trattamento dei dati sicuro. La sezione si chiude demandando la disciplina della "eredità digitale" al legislatore.

La sezione successiva, dal titolo di *Derechos de igualidad*, contiene cinque articoli. Oltre al diritto alla non discriminazione, al diritto all'accesso e al contrasto al divario digitale, la sezione prevede una ricca disposizione in merito alla protezione dei minori. Tale disciplina (art. X) si apre ponendo a carico dei soggetti responsabili (es. i genitori) il compito di assicurare un uso responsabile degli ambienti digitali per garantire il corretto sviluppo del minore. Tra le altre cose, l'articolo X prevede l'introduzione di procedure per la verifica dell'età, il diritto di ricevere una formazione e un'informazione adeguate alle capacità del minore e un generale divieto di trattamento dei dati personali dei minori a fini di profilazione.

La terza sezione della *Carta* contiene disposizioni in tema di partecipazione e di informazione tramite ambienti digitali. Essa si apre con il riferimento alla neutralità della rete Internet e prosegue poi affrontando il tema dell'informazione in ambiente digitale. In particolare, l'art. XV afferma il diritto a ricevere informazioni veritiere e conformi ai protocolli sulla trasparenza (in base ai quali comunicare se l'informazione è stata elaborata mediante processi automatizzati o se ha carattere pubblicitario o meno). La sezione in parola si conclude con tre articoli che affermano il diritto dei cittadini alla partecipazione politica per mezzi digitali, a ricevere un'educazione digitale e ad avere rapporti digitali con la pubblica amministrazione.

La quarta e la quinta sezione affrontano precise tematiche degli ambienti digitali. In una, si offrono indicazioni relative al rispetto dei diritti fondamentali dei lavoratori (art. XIX) e alla libertà di impresa in un contesto concorrenziale (art. XX) e nell'altra si prevedono disposizioni in materia di ricerca scientifica, diritto alla salute e diritto all'attività artistica-culturale, nonché in relazione all'impiego di programmi di intelligenza artificiale e di neuro-tecnologie. In tale quinta sezione, rubricata *Derechos digitales en entornos e specificos*, la *Carta* fa riferimento anche alla necessità dello sviluppo tecnologico di rispettare la sostenibilità ambientale e le generazioni future. La *Carta* si conclude con una sesta sezione, *Garantias y eficacia*, che riconosce la tutela dei diritti fondamentali anche in ambiente digitale.

Di tutta evidenza, la *Carta* si inserisce in una lunga lista di testi simili, adottati da altre autorità al fine di governare gli ambienti digitali affermando il rispetto dei diritti fondamentali. In tal senso, il testo spagnolo ricorda la *Dichiarazione dei diritti in Internet*, approvata dalla Camera dei Deputati nel 2015 e che conteneva già diverse disposizioni analoghe a quelle ora affermate nella *Carta* (*e.g.* neutralità della rete, inviolabilità dei sistemi informatici, protezione dell'anonimato).

DANIELE IMBRUGLIA

https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

2. La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell'algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di

un servizio di calcolo del c.d rating reputazionale)

Con l'ordinanza n. 14381/2021, la sezione I della Corte di Cassazione si è pronunciata sui requisiti di validità del consenso al trattamento dei dati personali degli aderenti a una piattaforma web volta ad elaborare i loro profili reputazionali attraverso un calcolo algoritmico (l'"**Ordinanza**"). Benché l'Ordinanza riguardi una vicenda antecedente alla entrata in vigore del Regolamento UE 2016/1679 ("**GDPR**"), essa presenta sicura rilevanza in materia per il principio in essa espresso che condiziona la validità della prestazione del consenso al trattamento dei dati personali alla conoscibilità dell'algoritmo che fa funzionare il servizio per il quale il consenso è prestato.

La vicenda trae origine dal provvedimento n. 488 del 24 novembre 2016 del Garante per la protezione dei dati personali ("**Garante Privacy**) con il quale era stata vietata qualunque operazione di trattamento dei dati personali effettuata dalla piattaforma web in questione, la piattaforma "MEVALUATE" (con connesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche. Attraverso tale piattaforma, l'associazione titolare del trattamento intendeva offrire un servizio idoneo a contrastare fenomeni basati sulla creazione di profili artefatti o inveritieri, affidando a un meccanismo di calcolo algoritmico la determinazione del c.d. "*rating* reputazionale" dei soggetti censiti. Obiettivo ultimo, pertanto, era quello di consentire a terzi interessati di poter verificare la reale credibilità di quei profili.

L'associazione Mevaluate Onlus si rivolgeva quindi al Tribunale di Roma chiedendo l'annullamento del provvedimento del Garante Privacy. Il ricorso trovava accoglimento quasi integrale da parte del Tribunale di Roma che con sentenza n. 5715/2018 del 4 aprile 2018 faceva salva l'efficacia del divieto solo in relazione al trattamento dei dati personali riguardi soggetti terzi non associati a Mevaluate Onlus.

La decisione del Tribunale veniva infine impugnata in Cassazione dal Garante.

Ai presenti fini, ciò che più interessa evidenziare è il fatto che la Corte di Cassazione si è allontanata dai temi maggiormente disputati (con esiti opposti) davanti al Garante e al Giudice di merito, ritenendo rilevante quello dei presupposti di validità del consenso al trattamento dei dati personali. Nel complesso motivazionale che aveva permesso al Tribunale di Roma di accogliere (pressoché integralmente) il ricorso contro il provvedimento del Garante, assumeva rilievo fondamentale la riflessione sull'attività oggetto del servizio "MEVALUATE". Il Tribunale di Roma osservava che non può negarsi all'autonomia privata la facoltà di organizzare sistemi di accreditamento di soggetti fornendo servizi "valutativi" per la conclusione di contratti e per la gestione di rapporti economici, a ciò non ostando – contrariamente da quanto ritenuto dal Garante a motivazione del suo provvedimento di divieto – neppure il difetto di una cornice normativa *ad hoc* in tema di *rating* reputazionale, stante la diffusione, nella realtà attuale, di fenomeni di valutazione e di certificazione da parte di privati a fini di attestazione di qualità e/o conformità a norme tecniche. Tanto premesso ed argomentato, il Tribunale di Roma considerava legittimo il trattamento dei dati personali dei soggetti aderenti al sistema "MEVALUATE", in quanto, nella specie, ritenuto validato dal loro consenso.

La Corte di Cassazione, nell'Ordinanza qui in commento, ha invece sottoposto ad analisi specifica i presupposti per la validità del consenso al trattamento dei dati personali.

A tal riguardo, la norma presa in considerazione dall'Ordinanza è l'art 23 d.lgs. n. 196/2003 ("**Codice Privacy**") nella versione antecedente all'entrata in vigore del GDPR (cfr. Cass., n. 16358/2018; Cass., n. 17278/2018). All'uopo, la Corte di Cassazione ricorda innanzitutto nell'Ordinanza in termini generali che occorre che il consenso non solo sia espresso dall'interessato in modo libero e con riguardo a uno specifico trattamento, ma, soprattutto, è necessario che l'oggetto della manifestazione di volontà sia un trattamento "chiaramente individuato" e documentato per iscritto. In particolare, la Corte evidenzia nell'Ordinanza lo stretto legame tra la manifestazione del consenso e il ruolo della informazione, e che un trattamento chiaramente individuato, per dirsi tale, presuppone che, a monte, il titolare del trattamento abbia provveduto a fornire le informazioni necessarie, ai sensi dell'art. 13 del Codice Privacy, individuandone gli elementi essenziali, gravando sul titolare l'onere di provare che il trattamento si fonda su un consenso idoneo e validamente ottenuto.

Ciò premesso, la Cassazione ha applicato i suddetti principi enunciati al caso di specie, reputando che – avuto riguardo alle caratteristiche tecnologiche del servizio (che si avvale di algoritmi di calcolo del rating reputazionale) e alla loro conoscibilità da parte degli interessati – la manifestazione del consenso prestata dagli aderenti alla piattaforma *de qua* non sia sufficiente a garantire la liceità del trattamento. Ciò in quanto, secondo la Cassazione, detto consenso si fonda su

informazioni opache rispetto all'algoritmo impiegato dalla piattaforma per il calcolo del rating. Tale aspetto costituisce un passaggio cruciale della decisione. A riguardo, la Corte precisa che la scarsa trasparenza dell'algoritmo impiegato non incide solo sul *"momento valutativo del procedimento"*, bensì sulla stessa liceità del trattamento, in quanto fondato su una base giuridica viziata. Sotto questo profilo, i giudici di legittimità contestano la decisione del tribunale di Roma, secondo il quale, i dubbi relativi al sistema automatizzato di calcolo del rating reputazionale non sarebbero decisivi, in quanto spetterebbe al mercato *«stabilire l'efficacia e la bontà del risultato ovvero del servizio prestato dalla piattaforma»*. Questo passaggio viene particolarmente criticato dai Giudici nomofilattici, in quanto, nella loro interpretazione, esso non coglie il cuore del problema, rappresentato dal consenso prestato dagli aderenti alla piattaforma. Secondo la Corte di Cassazione, invero, *«non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati»*. Tanto significa che la Corte ammette, in generale, la possibilità di sviluppare servizi di "rating reputazionale" basati su consenso dell'interessato, ma se l'algoritmo e gli elementi di cui si compone restano ignoti o non sono conoscibili da parte degli interessati, il requisito della consapevolezza non può dirsi soddisfatto.

In questa prospettiva, la sentenza di merito veniva dunque cassata e rinviata al medesimo Tribunale di Roma, in diversa composizione, per un nuovo esame da condursi osservando il seguente principio di diritto: «*In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati*».

SALVATORE ORLANDO / CHIARA SARTORIS

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5796783
https://web.uniroma1.it/deap/sites/default/files/allegati/CASO_MEVALUATE_02.pdf
https://web.uniroma1.it/deap/sites/default/files/allegati/CASO_MEVALUATE_03.pdf

3. Il pronunciamento congiunto EDPS - EDPB del 21 giugno 2021 sulla proposta di disciplina sul riconoscimento facciale contenuta nell'Artificial Intelligence Act

Il 21 giugno 2021 l'EDPB (*European Data Protection Board*) e l'EDPS (*European Data Protection Supervisory*) hanno adottato un'opinione congiunta sulla proposta di regolamento europeo per l'Intelligenza Artificiale ("*Artificial Intelligence Act*" o "**AIA**") presentata dalla Commissione europea il 21 aprile 2021 (su cui v. la notizia n.1 sul numero 2/2021 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf). Pur accogliendo positivamente l'iniziativa della Commissione di regolamentare l'utilizzo dell'intelligenza artificiale nell'ambito dell'UE e l'adozione di un approccio basato sul rischio (*risk-based*), le due Autorità hanno evidenziato alcune criticità in merito alla proposta.

Innanzitutto, l'EDPS e l'EDPB sottolineano la necessità di specificare chiaramente che tutti i trattamenti di dati personali effettuati attraverso sistemi di intelligenza artificiale rientrano nell'ambito di applicabilità – oltre che dell'AIA – della normativa europea in materia di protezione dei dati. Ne consegue che un sistema di IA che implica un trattamento di dati personali, pur rispettando le condizioni previste dalla medesima proposta di regolamento, non può considerarsi lecito e non può essere introdotto nel mercato europeo se non risulta conforme alla normativa sulla protezione dei dati personali. Inoltre, il concetto di "rischio per i diritti fondamentali" deve essere allineato a quello utilizzato nel GDPR al fine di assicurare un quadro normativo europeo coerente ed armonizzato.

L'EDPS e l'EDPB si sono poi focalizzati sull'utilizzo di sistemi di IA per la rilevazione, il riconoscimento e l'analisi dei dati biometrici. In particolare, in linea con quanto già espresso dall'EDPS in un comunicato stampa del 23 aprile 2021 (su cui v. la notizia n.2 sul numero 2/2021 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf), le Autorità hanno chiesto l'introduzione di un divieto totale all'uso dell'IA per l'identificazione biometrica a distanza in spazi pubblicamente

accessibili attraverso il riconoscimento automatico di caratteri biometrici o comportamentali come il volto, la voce, l'andatura, il modo di scrivere su una tastiera, le impronte digitali e il DNA, che farebbe venire meno ogni forma di anonimato in questi spazi. Allo stesso modo, il divieto dovrebbe riguardare l'utilizzo dell'IA per la creazione, attraverso l'analisi dei dati biometrici, di *cluster* in cui gli individui sono raggruppati sulla base di caratteristiche potenzialmente discriminatorie come l'etnia, il genere, l'orientamento politico e sessuale o sulla base di qualsiasi altro fattore di discriminazione vietato ai sensi dell'art. 21 della Carta dei diritti fondamentali dell'Unione Europea. Infine, l'uso di sistemi di IA dovrebbe essere vietato per la rilevazione delle emozioni delle persone fisiche (salvo casi particolari in cui tale utilizzo può avere effetti positivi sugli individui, ad esempio in ambito sanitario) e per l'assegnazione di qualsiasi tipo di *social scoring*. In particolare, i Presidenti delle due Autorità (Andrea Jelinek per l'EDPB e Wojciech Wiewiórowski per l'EDPS) hanno segnalato che tali utilizzi dell'IA andrebbero a minare nelle loro fondamenta i diritti e le libertà fondamentali riconosciuti e tutelati dall'UE (come il diritto alla libertà personale e il divieto di discriminazioni), e per questo si rende necessario un approccio precauzionale attraverso l'introduzione di un divieto generale al fine di garantire uno sviluppo dell'IA e un sistema normativo che pongano al centro l'essere umano (*human-centric*).

Gli ultimi punti affrontati nell'*opinion* riguardano il quadro istituzionale, a partire dalla previsione della proposta di AIA per la quale, nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione Europea rientrano nell'ambito di applicazione dell'AIA, l'EDPS agirebbe in qualità di autorità di vigilanza del mercato. Le Autorità richiedono che la proposta specifichi in maniera più dettagliata la portata del ruolo e dei compiti assegnati all'EDPS in qualità di autorità di vigilanza del mercato. In secondo luogo, richiedono che le autorità di controllo nazionali per la protezione dei dati siano designate quali autorità nazionali di controllo ai sensi dell'Art. 59 della proposta di AIA. Tali autorità, infatti, occupandosi già di tutelare i diritti fondamentali e di vigilare sul rispetto del GDPR e della Direttiva UE 2016/680 c.d. Law Enforcement Directive ("LED") per i trattamenti di dati personali che coinvolgono sistemi di IA, potrebbero assicurare che l'interpretazione e l'applicazione dell'emanando regolamento sull'IA sia omogenea in tutti gli Stati Membri e sia coerente con la normativa sulla protezione dei dati personali. Infine, le Autorità hanno criticato il ruolo dominante che la proposta di regolamento prevede di attribuire alla Commissione europea nell'istituendo *European Artificial Intelligence Board* (EAIB) sostenendo che tale ultimo organo, per svolgere adeguatamente le proprie funzioni, dovrebbe essere indipendente dal potere politico e godere di una maggiore autonomia di iniziativa.

CHIARA RAUCCIO

https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

4. Le regole sul riconoscimento facciale per le società private emesse dalla Suprema Corte del Popolo della Repubblica Popolare Cinese il 28 luglio 2021.

Il 28 luglio 2021, la Suprema Corte del Popolo della Repubblica Popolare Cinese ha pubblicato il *Provvedimento della Corte Suprema del Popolo su diverse questioni relative all'applicazione della legge nei procedimenti civili relativi all'uso della tecnologia di riconoscimento facciale per il trattamento delle informazioni personali* (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定, in seguito il 'Provvedimento'). Il documento costituisce, dal punto di vista del sistema delle fonti cinese, un'interpretazione giudiziale autentica, a cui è riconosciuto valore di legge e con cui la Suprema Corte è solita fissare norme e principi per la corretta applicazione delle leggi. In particolare, il Provvedimento di cui al presente commento, è composto da 16 articoli ed è pubblicato, si legge, allo scopo di 'implementare lo stato di diritto di Xi Jinping, porre al centro del sistema la persona, salvaguardare i diritti della personalità delle persone fisiche e proteggere la sicurezza dei volti dei cittadini'. Con esso la Corte Suprema 'si fa carico dei principi contenuti nel nuovo codice civile, allo stesso tempo rafforza la tutela giudiziale delle informazioni personali (fra i quali, ovviamente, il volto non può che essere sussunto nella categoria) e promuove lo sviluppo sano dell'economia digitale'. La pubblicazione ha notevole rilievo, oltre che per la sua incidenza nomofilattica, anche per la sua sostanziale portata innovativa. Esso mira a rafforzare la tutela giuridica delle informazioni sensibili, vale a dire, quelle informazioni personali che, ai sensi dei *National Standard of Information Security Technology – Personal Information Security Specification* (信息安全技术 个人信息安

全规范), sono da considerarsi come potenzialmente dannose per la sicurezza degli individui e quindi oggetto di tutela rafforzata da parte dell'ordinamento. Tra le informazioni sensibili rientrano appunto le informazioni 'biometriche', vale a dire i tratti fisiognomici delle persone fisiche e che, quindi, sono oggetto di tutela rafforzata. Ma vediamo come impatta, a livello prescrittivo, il Provvedimento. Esso prevede alcune fattispecie illecite, che violano la legge sulla protezione delle informazioni personali. Esse sono: l'utilizzo di tecnologie di riconoscimento facciale per la verifica, il riconoscimento o l'analisi del volto in aree pubbliche (ad esempio, hotel, centri commerciali, banche, stazioni, aeroporti, stadi, etc.), in contrasto con disposizioni di legge; mancata comunicazione delle regole per il trattamento dei dati personali o mancata esplicitazione delle finalità, modalità o perimetro del trattamento; mancato ottenimento del consenso dell'interessato; trattamento di informazioni biometriche in difformità dal consenso ricevuto; mancata adozione delle misure di sicurezza obbligatorie per legge; fornitura di informazioni biometriche a terzi; utilizzo delle informazioni biometriche in violazione dell'ordine pubblico; trattamento delle informazioni biometriche in violazione dei principi di legalità, legittimità e necessità. Un'ulteriore novità è costituita dal fatto che per il trattamento delle informazioni biometriche sarà necessario richiedere, da parte del titolare del trattamento, ed ottenere, da parte del soggetto le cui informazioni sono raccolte, un consenso 'specifico' per questo tipo di informazioni. Il Provvedimento ha iniziato a dispiegare i suoi effetti a partire dal 1° agosto 2021.

CORRADO MORICONI

http://www.court.gov.cn/fabu-xiangqing-315851.html

5. Le Linee Guida EDPB del 7 luglio 2021 sugli assistenti vocali virtuali.

Il 7 luglio 2021 il Comitato europeo per la protezione dei dati personali, *European Data Protection Board* (l'"**EDPB**"), ha adottato la versione definitiva, successiva a pubblica consultazione, delle Linee Guida sugli assistenti vocali virtuali - *Guidelines on virtual voice assistants* (le "**Linee Guida**").

L'assistente vocale virtuale (*Virtual Voice Assistant*: "**VVA**") è un programma che interpreta il linguaggio naturale tramite algoritmi di intelligenza artificiale capace di interloquire con gli esseri umani allo scopo di soddisfare le relative richieste o di compiere determinate azioni. Così, un VVA è in grado di effettuare ricerche di informazioni, di perfezionare acquisti *online*, di far ascoltare brani musicali, ma anche, nel contesto domotico - che rappresenta terreno privilegiato di applicazione di simili soluzioni - di regolare la temperatura o l'illuminazione dell'ambiente, di attivare elettrodomestici o allarmi ecc. I VVA trovano il loro supporto fisico in un dispositivo terminale dotato di microfoni e altoparlanti: un *computer*, uno *smartphone*, una *smart tv*, un *tablet* o un *device* autonomo come lo *smart speaker*.

L'EDPB, nella consapevolezza della notevole diffusione che negli ultimi anni i VVA hanno vissuto, all'interno di uno scenario ormai connotato da un avvento massiccio del digitale, raccomanda l'adozione di soluzioni conformi alla normativa europea vigente in materia di trattamento dei dati personali e di comunicazioni elettroniche.

In effetti, le Linee Guida affrontano in maniera assai definita una pluralità di aspetti relativi ai dispositivi in questione, dei quali viene delineata una definizione ed una rappresentazione dettagliata che descrive i meccanismi tecnologici sottostanti al loro funzionamento. Soprattutto, vengono evidenziati i rischi che ne derivano per gli utenti e le sfide che si profilano su un piano di *compliance* normativa.

Le Linee Guida pongono bene in luce fin da subito come sia intrinseco al funzionamento dei VVA l'accesso ad un'enorme quantità di dati personali, ivi inclusi tutti i comandi vocali degli utenti, ed al contempo come tali dati subiscano trasferimenti ai *server* remoti dei VVA stessi, con conseguente necessità di tenere in considerazione, per gli operatori che forniscono servizi di VVA, sia il Regolamento 2016/679 UE (il "**GDPR**") che la Direttiva 2002/58 CE (la "**direttiva e-Privacy**"): viene così delineata la cornice normativa di riferimento.

Con specifico riguardo alla direttiva e-Privacy, le Linee Guida ricordano che poiché i VVA operano sempre attraverso uno dei suddetti dispositivi fisici (*smartphone*, *tablet*, *smart speaker* ecc.), essi utilizzano reti di comunicazione elettronica per accedere a questi *device*, che costituiscono "apparecchiature terminali" nel senso della direttiva e-Privacy. Di conseguenza, le disposizioni dell'art. 5, par. 3 della direttiva e-Privacy si applicano ogni volta che il VVA memorizza o accede ad informazioni nel dispositivo fisico ad esso collegato. In base a tale previsione, l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso ad informazioni

archiviate nell'apparecchio terminale di un abbonato o di un utente deve essere consentito unicamente a condizione che l'interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento, e che gli sia offerta la possibilità di rifiutare tale trattamento.

Qualsiasi operazione di trattamento di dati personali conseguente, compreso il trattamento dei dati personali ottenuti accedendo alle informazioni nell'apparecchiatura terminale, deve inoltre avere una base giuridica ai sensi dell'art. 6 GDPR per essere lecita. Poiché il titolare del trattamento, quando richiede il consenso per la conservazione o l'accesso alle informazioni ai sensi dell'art. 5, par, 3, direttiva e-Privacy, dovrà informare l'interessato su tutte le finalità del trattamento, il consenso sarà generalmente la base giuridica più adeguata a coprire il trattamento conseguente dei dati personali. Quindi il consenso costituirà probabilmente, secondo le Linee Guida, la base giuridica sia per la memorizzazione e l'ottenimento dell'accesso a informazioni già memorizzate, che per il trattamento dei dati personali successivo a tali operazioni.

Inoltre, l'EDPB ricorda che, nell'individuazione della base giuridica appropriata, è obbligo dei titolari del trattamento tenere in ogni caso conto dell'impatto che si possa produrre sui diritti degli interessati e che l'art. 6 GDPR non può essere invocato dai *data controller* al fine di ridurre la protezione aggiuntiva fornita dall'art. 5, par. 3 direttiva e-Privacy. Quest'ultima, d'altronde, costituisce una *lex specialis* destinata a prevalere sul GDPR (come già stabilito nel Parere dello stesso EDPB 5/2019 sull'interazione tra la direttiva e-Privacy e il GDPR, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati).

Altro profilo a cui le Linee Guida dedicano attenzione riguarda l'eventualità che gli VVA registrino accidentalmente l'audio di soggetti terzi che non avevano intenzione di utilizzare i relativi servizi. Dal momento che appare altamente improbabile che un'attivazione accidentale possa essere interpretata come un consenso valido dell'interessato, i dati così raccolti dovrebbero essere cancellati.

Le Linee Guida tengono ulteriormente in considerazione le complicanze che derivano dalla presenza, sullo scenario determinato dall'operatività di un VVA, di una pluralità e una concatenazione di "attori" ('fornitore', 'progettista', 'sviluppatore', 'integratore', 'proprietario', 'utente', come definiti, rispettivamente, nelle Linee Guida) il che rende difficoltosa l'individuazione dei soggetti del trattamento dei dati personali e la conseguente ripartizione di obblighi e responsabilità, nonché l'identificabilità, da parte dell'interessato, dei soggetti coinvolti al fine del corretto esercizio dei suoi diritti. Pur in tale scenario complesso, secondo le Linee Guida si può comunque prospettare a carico del fornitore dei servizi VVA almeno l'obbligo di rilasciare idonea informativa conforme al GDPR non solo agli utenti registrati ai servizi VVA, ma anche a chi non è registrato e possibilmente persino agli utenti c.d. accidentali.

Quanto alla *data retention*, l'EDPB ricorda che in conformità al principio di limitazione della conservazione dei dati di cui al GDPR, i VVA dovrebbero conservare i dati per un tempo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati. Pertanto, i periodi di conservazione dei dati dovrebbero essere legati alle diverse finalità di trattamento.

Ancora, l'EDPB fa notare come fra i dati personali trattati dai VVA vi siano dati rientranti nelle categorie particolari *ex* art. 9 GDPR. In particolare, in questo contesto le Linee Guida osservano che gli stessi dati vocali sono intrinsecamente dati biometrici, richiamando la relativa definizione contenuta nell'art. 4(14) GDPR.

Dato che alcuni VVA hanno la capacità e la specifica funzione di identificare univocamente gli utenti solo in base alla loro voce, attraverso un metodo che si avvale della creazione di modelli di voce (c.d. *voice model recognition* o *voiceprint recognition*), il trattamento dei dati vocali in questi casi richiederà il consenso esplicito della/e persona/e interessata/e (art. 9, par. 2, lett. a) GDPR). Nell'ottenere il consenso degli interessati i titolari del trattamento dovranno rispettare le condizioni dell'art. 7 GDPR e, come chiarito nel Considerando 32 GDPR, dovrebbero offrire un metodo di identificazione alternativo alla biometria, in ossequio alla natura libera del consenso.

Sempre con riferimento alle applicazioni che utilizzano sistemi di *voice model recognition*, si profila il rischio concreto che i VVA operino la registrazione della voce di tutte le persone che parlano nell'ambiente interessato, al fine di riconoscere, attraverso il metodo del confronto con il modello di voce creato, la voce dello specifico e solo utente deputato a pronunciare la parola chiave di accensione del dispositivo. Le Linee Guida, pur ammettendo la necessità (ove regolarmente dichiarata ed assentita) per l'utente di essere vocalmente riconosciuto dal VVA, chiariscono che - onde evitare raccolte di dati biometrici che abbiano luogo all'insaputa di terzi ignari interessati - occorrerà privilegiare soluzioni tecniche di riconoscimento basate sui soli dati dell'utente stesso. Ciò implicherà la necessità di attivare il

riconoscimento biometrico solo ad ogni utilizzo che avvenga su iniziativa dell'utente che richieda di volta in volta l'identificazione, e non sulla base di un'analisi permanente delle voci ascoltate dal VVA. In tal senso, l'EDPB suggerisce ad es. che il VVA chieda all'utente se vuole essere identificato e che attenda una risposta positiva per attivare il trattamento biometrico.

Inoltre, molte delle raccomandazioni espresse dall'EDPB evidenziano la necessità di implementare adeguate misure di sicurezza e di rispettare la c.d. *privacy by design* e la *privacy by default*, in ossequio al principio di *accountability* che, come noto, permea l'intero tessuto normativo del GDPR. Ciò richiede che i fornitori e gli sviluppatori di VVA operino scelte idonee in termini appunto di *design* dei dispositivi, considerando *in primis* la necessità di avere o meno un utente registrato per ciascuna delle loro funzionalità. Ad es. per fare una ricerca su Internet, le Linee Guida ritengono che non sia strettamente necessario che l'utente sia registrato. In particolare, l'EDPB evidenzia come *di default*, i servizi che non richiedono un utente identificato non dovrebbero associare alcuno degli utenti identificati ai comandi. Inoltre, un VVA che sia rispettoso della *privacy by default* e *by design* dovrebbe elaborare solo i dati degli utenti per eseguire le richieste degli utenti e non memorizzare né i dati vocali né un registro dei comandi eseguiti. Ancora, i fornitori di VVA dovrebbero sviluppare standard industriali che consentano la portabilità dei dati in conformità con l'art. 20 GDPR e dovrebbero altresì garantire che tutti i dati degli utenti possano essere cancellati su richiesta dell'utente, conformemente all'art. 17 GDPR.

D'altronde, la garanzia dei diritti dell'interessato occupa a sua volta una parte assai sostanziosa delle Linee Guida, che ne vaglia l'applicabilità in concreto. Soprattutto viene dedicata attenzione proprio al "nuovo" diritto alla portabilità dei dati personali, per la piena applicazione del quale, nel contesto di un mercato unico digitale, i progettisti di VVA sono chiamati, secondo l'EDPB, a sviluppare formati comuni che facilitino l'interoperabilità tra i sistemi VVA.

LAVINIA VIZZONI

https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf

6. Le Linee Guida del Garante Privacy italiano sui cookies ed altri strumenti di tracciamento del 10 giugno 2021

Il 10 giugno 2021 il Garante per la protezione dei dati personali (il "**Garante**") ha adottato il provvedimento n. 231 – pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021 – recante le nuove "Linee guida *cookie* e altri strumenti di tracciamento" (le "**Linee Guida"**). Il provvedimento, che si applica non solo ai *cookie* ma a tutti gli strumenti di tracciamento attivi e passivi (es. *fingerprinting*), ha confermato sotto diversi aspetti le precedenti posizioni del Garante – espresse in particolare nelle linee guida sui *cookie* del 2014 – e ha introdotto alcune significative novità.

In primo luogo, viene confermata la distinzione tra *cookie* di prima parte (posizionati dal sito web visitato dall'utente) e *cookie* di terze parti (posizionati da siti o web server diversi). Altra classificazione, basata sulla funzione svolta e a cui si collega una diversa disciplina applicabile, è quella dei *cookie* tecnici (necessari per la stessa erogazione del servizio offerto all'utente tramite il sito web), *cookie analytics* (equiparati ai *cookie* tecnici se utilizzati esclusivamente per produrre statistiche aggregate senza la possibilità di risalire all'utente) e *cookie* di profilazione (utilizzati per ricondurre agli utenti specifiche azioni o schemi comportamentali al fine di raggrupparli in *cluster* omogenei così da personalizzare la fornitura del servizio e inviare messaggi pubblicitari mirati, in linea con le preferenze manifestate dall'utente durante la navigazione in rete).

Il Garante ha poi precisato che la normativa applicabile agli strumenti di tracciamento è l'art. 122 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, il "**Codice Privacy**") che ha dato attuazione nel nostro ordinamento alla direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (la "**direttiva ePrivacy**"). Il regolamento (UE) 2016/679 ("**GDPR"**) ha invece un ambito di applicazione residuale limitato ai profili non direttamente disciplinati dall'art. 122 del Codice Privacy. La direttiva ePrivacy, infatti, si configura come *lex specialis* rispetto al GDPR e, pertanto, è destinata a prevalere su quest'ultimo per la parti di potenziale sovrapposizione. Ne deriva un'importante conseguenza, cioè che il trattamento dei dati personali attraverso gli strumenti di tracciamento può avvenire esclusivamente sulla base del consenso salvi i casi per i quali la direttiva ePrivacy

stabilisce che il consenso non è necessario – mentre non può fondarsi sulle altre basi giuridiche previste dal GDPR ma non dalla direttiva ePrivacy (tra cui, in particolare, il legittimo interesse).

Il Garante si sofferma poi sulle modalità di acquisizione del consenso online. Un primo riferimento è allo *scrolling* per il quale le Linee Guida, confermando la posizione espressa dall'EDPB (*European Data Protection Board*) nel parere n. 5/2020 del 4 maggio 2020 (su cui v. la notizia n. 5 sul numero 2/2020 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf), chiariscono che di per sé lo *scrolling* non costituisce un metodo idoneo alla raccolta del consenso, ma può divenire ammissibile se inserito nell'ambito di un processo più articolato tale da assicurare che la scelta dell'interessato sia inequivoca, consapevole, registrabile e documentabile. Altro tema è quello del c.d. *cookie wall* che il Garante definisce un meccanismo vincolante non conforme al requisito di libertà del consenso, salva l'ipotesi nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di *cookie* o altri strumenti di tracciamento, aggiungendo tuttavia che occorre valutare caso per caso se il titolare del trattamento offra una simile possibilità di accedere ad un contenuto o un servizio equivalente per il quale non sia necessario accettare l'installazione di *cookie*. Anche questo tema era stato affrontato nel richiamato parere dell'EDPB n. 5/2020 del 4 maggio 2020 (su cui v. la notizia n. 5 sul numero 2/2020 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf). Resta peraltro aperta la questione di cosa debba intendersi per "servizio equivalente" e da che punto di vista – oggettivo o soggettivo – debba valutarsi l'equivalenza.

Un'importante novità riguarda il divieto di reiterazione della richiesta di consenso ad ogni accesso dell'utente al sito web, che il Garante definisce "ridondante e invasiva" e come tale lesiva della libertà di scelta dell'interessato. Ci sono solo tre casi in cui la reiterazione è ammessa: (i) mutamento significativo delle condizioni del trattamento; (ii) impossibilità per il gestore del sito di sapere che un *cookie* è stato già installato (ad esempio perché l'utente ha cancellato i *cookie*); (iii) dopo 6 mesi dalla precedente richiesta.

Il Garante approfondisce infine il principio della *privacy by design* e *by default* in applicazione del quale il sito web deve essere configurato in modo che al primo accesso dell'utente non sia installato alcun *cookie* e compaia un *banner* contenente alcune informazioni minime sull'utilizzo dei *cookie*. Il *banner* deve rappresentare una discontinuità nella fruizione del servizio in modo che l'utente possa facilmente identificarlo, e deve essere configurato in modo da non ingannare l'utente cercando di forzare o manipolare le sue scelte (ad esempio attraverso l'uso di colori o dimensioni dei caratteri che spingano l'utente a premere il pulsante di accettazione dei *cookie*). In particolare, l'utente deve avere la possibilità di rifiutare agevolmente i *cookie* anche semplicemente chiudendo il *banner* e, in ogni momento, deve essere in grado di modificare le scelte compiute accedendo ad un'apposita sezione del sito. Solo nel caso in cui il sito utilizzi esclusivamente *cookie* tecnici – o *cookie* analitici equiparati a quelli tecnici – non si rende necessario uno specifico banner ma è sufficiente inserire l'informativa per i *cookie* nella *homepage* o all'interno dell'informativa generale del sito.

CHIARA RAUCCIO

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876

7. La decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un "euro digitale".

Il 14 luglio 2021 il Consiglio direttivo della Banca centrale europea ("**BCE**") ha comunicato la decisione di avviare il progetto per un "euro digitale". Il progetto avrà inizio nel mese di ottobre 2021 con una fase di analisi della durata di due anni.

La fase di analisi verterà sulla configurazione e sulle modalità di distribuzione di un euro digitale, nonché sul relativo impatto sul mercato e sui rischi per la *privacy* e per l'economia dell'area euro. Riguarderà, in aggiunta, le modifiche legislative che potrebbero rendersi necessarie e implicherà il confronto della BCE con i responsabili delle politiche europee. Un nuovo gruppo consultivo di mercato, il *Digital Euro Market Advisory Group* ("**MAG**"), terrà conto dei punti di vista degli utenti e dei distributori, i quali saranno poi discussi anche dal già esistente *Euro Retail Payments Board* ("**ERPB**"), che, sin dal 2013, ha lo scopo di favorire l'integrazione, innovazione e competitività dei pagamenti al dettaglio in euro. Al termine, la BCE deciderà circa l'effettivo sviluppo di un euro digitale.

La fase di analisi fa seguito alle precedenti attività della BCE condotte al riguardo, fra cui il "Rapporto su un euro digitale" pubblicato nel quarto trimestre del 2020 ("**Rapporto**"). Nel Rapporto sono stati delineati i principi generali a cui l'ideazione di un euro digitale dovrebbe ispirarsi e i requisiti che dovrebbe soddisfare. Secondo i principi delineati, l'euro digitale dovrebbe rappresentare una passività della banca centrale offerta in forma digitale e dovrebbe fungere da complemento al contante e alle soluzioni di pagamento private. Costituirebbe, quindi, un'altra forma attraverso cui rappresentare l'euro e non una valuta ulteriore. L'emissione, poi, dovrebbe aversi garantendo accessibilità e coesistenza con soluzioni di pagamento private per i pagamenti digitali *retail*, nonché fiducia da parte degli utenti finali. I requisiti sono stati definiti con riferimento sia a specifici scenari che potrebbero motivarne l'emissione, sia ai potenziali effetti che un euro digitale potrebbe avere. In generale, fra tutti, si hanno sicurezza e solidità; fruibilità; efficienza; cooperazione con gli operatori di mercato; conformità al quadro regolamentare.

Dalla configurazione dell'euro digitale ne dipende il fondamento normativo. A seconda che sia concepito per un impiego circoscritto a determinate fattispecie o per un uso diffuso, la base giuridica sarà diversa. Come evidenziato dal Rapporto, l'alternativa coerente a un impiego diffuso e analogo al contante- che sembrerebbe essere l'ipotesi prevalente- sarebbe data da l'art. 128, co. 1, TFEU e l'art. 16 dello Statuto del SEBC, secondo cui le banconote in euro emesse dall'Eurosistema sono le uniche banconote aventi corso legale nell'Unione. Secondo il Rapporto, l'assenza di un'espressa previsione che escluda la possibilità per l'Eurosistema di emettere strumenti aventi corso legale diversi dalle banconote e la mancanza di disposizioni circa il mezzo e il formato attraverso cui dovrebbe avvenire l'emissione delle *euro banknotes* consentirebbero margini di discrezionalità nell'emissione di un euro digitale.

Le sfide tecnologiche poste da un euro digitale sono state valutate nel successivo lavoro di sperimentazione condotto dall'Eurosistema congiuntamente a esponenti del mondo accademico e del settore privato. Per ciascun *work stream*, diversi assetti di emissione e distribuzione, centralizzati e non, sono stati presi in esame. In particolare, si sono considerate, in combinazione o alternativamente, sia soluzioni basate su infrastrutture esistenti e su sistemi *account-based*, sia tecnologie innovative e sistemi *distributed ledger-based*. In aggiunta, sono state prese in esame soluzioni *offline*. La valutazione è stata condotta rispetto a quattro ambiti: tecnologia per un euro digitale (*digital euro ledger*); *privacy* e contrasto al riciclaggio di denaro; limiti alla circolazione di un euro digitale; accessibilità da parte degli utenti. Dalle risultanze ottenute è emerso che non vi dovrebbero essere ostacoli allo sviluppo di un euro digitale per nessuna delle aree considerate. Le evidenze emerse costituiranno una prima base per la fase di analisi.

La fase di indagine terrà conto anche della consultazione pubblica condotta in parallelo al lavoro di sperimentazione. Dalle risposte ottenute è emerso che l'aspetto che i cittadini e i professionisti ritengono più rilevante nello sviluppo di un euro digitale è la *privacy*, anche se altrettanta rilevanza è stata attribuita alla prevenzione di attività illecite. Particolare attenzione è stata dedicata anche al tema della sicurezza e dell'accessibilità, nonché alla possibilità di utilizzare l'euro digitale senza costi aggiuntivi e *offline*. Rispetto alle modalità di distribuzione, è emersa una preferenza per un'integrazione dell'euro digitale negli attuali sistemi bancari e di pagamento, con, però, anche il desiderio di godere di servizi aggiuntivi.

ALICE FILIPPETTA

https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.it.html
https://www.ecb.europa.eu/paym/digital_euro/mag/shared/files/digital_euro_stakeholder_engagement.pdf
https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

8. La Repubblica di El Salvador adotta il Bitcoin come moneta avente corso legale nel Paese (la "Ley Bitcoin" dell'8 giugno 2021).

Attraverso il decreto 57/2021 del 9 giugno 2021 (noto come "**Ley Bitcoin**"), l'Assemblea Legislativa della República de el Salvador ha introdotto il Bitcoin come "moneda de curso legal" rendendo, di fatto, lo Stato centroamericano il primo paese al mondo a adottare la più diffusa cryptomoneta come valuta domestica. Il provvedimento, già preannunciato dal Presidente Nayid Bukele qualche settimana prima della sua presentazione, avrà efficacia decorsi 90 giorni dalla votazione della proposta in Parlamento e, segnatamente, il 7 settembre 2021. Oltre a ragioni legate all'opportunità di attrarre investimenti stranieri, le caratteristiche del sistema economico e finanziario dello Stato centroamericano sono state

alla base di una scelta così radicale ed innovativa, nonché della larga maggioranza con la quale essa è stata votata in Parlamento (64 voti su 84 totali).

El Salvador appartiene a quegli ordinamenti che nell'esercizio della propria sovranità monetaria decidono di riconoscere – in via esclusiva o in aggiunta ad una o più valute locali – corso legale ad una moneta emessa da un ordinamento straniero. La scelta risiede perlopiù nella volontà di una economia in via di sviluppo di incrementare gli scambi commerciali con l'estero attraverso una riduzione del rischio di cambio, che altrimenti disincentiverebbe investitori stranieri nel fare affidamento a valute più deboli (come nel caso del Colon salvadoregno). Nel caso della Repubblica centroamericana, già prima del 2001, questo obiettivo era comunque perseguito attraverso un regime di cambio fisso fra la valuta locale ed il dollaro USA; a seguito poi dell'entrata in vigore della "Ley de Integracion Monetaria" (Ley 201 del 30 novembre 2000), è stato poi riconosciuto al dollaro americano valore di moneta avente corso legale nello Stato. La situazione di costante instabilità politica e l'alto tasso di criminalità della República non ha però consentito di raggiungere gli effetti sperati, producendo al contrario un aumento vertiginoso dell'inflazione ed ampliando il divario di ricchezza fra le diverse fasce della popolazione. L'adozione della valuta americana come moneta domestica implicava, inoltre, una significativa riduzione dei margini di manovra del Banco Central de Reserva de el Salvador, poiché rendeva lo Stato dipendente dalle decisioni di politica monetaria intraprese dall'organo che regola l'emissione della valuta americana (il Federal Reserve System). La crisi derivante dalla diffusione della pandemia da COVID-19 ha poi ulteriormente acutizzato il problema della dipendenza dalla sovranità monetaria di uno Stato estero. Per far fronte alla crisi dell'economia reale indotta dalle chiusure forzate delle attività non essenziali, il FED ha iniettato nel sistema finanziario dosi di liquidità elevata che hanno determinato, nei Paesi con economie "satellite" di quella americana, un aumento incontrollabile delinflazione.

La nuova legge si colloca così - per espressa menzione all'interno dei considerando iniziali - sotto l'egida dell'art. 102 della Constitución de la República, la quale attribuisce allo Stato il compito di promuovere e sostenere l'iniziativa privata, generando le condizioni necessarie per accrescere la ricchezza nazionale a beneficio del maggior numero di abitanti possibile. Il riconoscimento del Bitcoin come moneta avente corso legale nasce difatti come manovra di finanza inclusiva, tenuto conto del fatto che circa il 70% della popolazione non ha accesso a servizi finanziari tradizionali e che una parte significativa degli introiti finanziari dello Stato (attorno al 22% del PIL) provengono da proventi inviati da cittadini salvadoregni al proprio Paese d'origine. Su queste basi, la legge dispone la regolamentazione del Bitcoin come moneta a corso legale, con potere liberatorio senza alcuna restrizione, senza alcun limite in ogni transazione e a qualsiasi titolo che le persone fisiche o giuridiche, pubbliche o private richiedano di compiere (art. 1). A livello di mercato interno, il Bitcoin potrà essere impiegato per esprimere i prezzi di beni e servizi (art. 3), per adempiere ad obblighi tributari (art. 4), con obbligo per ogni agente economico di accettare la cryptovaluta come forma di pagamento (art. 7). Le disposizioni della Ley Bitcoin assumono dunque, ad oggi, carattere meramente programmatico, richiamando il compito dello Stato di fornire alternative che consentano agli utenti di effettuare transazioni in Bitcoin, di garantire convertibilità automatica ed istantanea fra Bitcoin e dollari (art. 8), di promuovere la formazione e i meccanismi di accesso della popolazione a transazioni in Bitcoin (art. 12), oltre ad affidare all'Esecutivo, al Banco Central e alla Sovrintendenza al Sistema Finanziario la competenza ad adottare i regolamenti attuativi (artt. 10 e 11). Prima dell'entrata in vigore della legge, lo Stato garantirà inoltre la convertibilità automatica ed istantanea fra dollaro e Bitcoin attraverso la creazione di un trust nella Banca di Sviluppo di El Salvador (art. 14). La legge produce infine, per espressa previsione, efficacia retroattiva, riconoscendo la facoltà di adempiere in Bitcoin ogni obbligazione pecuniaria in essere espressa in dollari (art. 13).

Al netto delle implicazioni "politiche" che questa decisione assume – rendendo el Salvador frontrunner di un esperimento che sarà verosimilmente emulato da parte di altri ordinamenti – la scelta di adottare il Bitcoin come valuta domestica produce rilevanti implicazioni sul versante della politica monetaria e dell'ordine giuridico interno dello Stato. Sotto il primo aspetto, è noto che una delle principali caratteristiche della cryptovaluta è quella per cui il suo valore non è fissato o influenzato dalle scelte di uno Stato, una banca centrale o un intermediario finanziario (moneta FIAT), ma dipende – in larga parte – da "criterios de libre mercado" (così il considerando V della Ley Bitcoin), secondo un sistema cd. decentralizzato. In buona sostanza, la sua produzione ed immissione nel sistema non dipende da una programmazione di un ente centrale in considerazione di obiettivi di politica monetaria, bensì dalla progressione dell'attività di mining

scandita da un algoritmo (fino all'ammontare massimo di 21 milioni previsto dal protocollo Bitcoin entro il 2140). Se dunque, da un lato, il fondamento di politica economica che ha sorretto la scelta della República de el Salvador è stato quello di sottrarsi all'influenza prodotta delle decisioni monetarie del FED, dall'altro, il riconoscimento di corso legale al Bitcoin non comporta alcun recupero di sovranità monetaria da parte dello Stato, poiché le decisioni del Banco Central hanno una più limitata capacità di incidere sull'economia reale rispetto a fattori legati all'andamento di mercato della cryptovaluta. Sotto un secondo aspetto, l'adozione del Bitcoin come unità di conto e mezzo di scambio comporta l'obbligo del creditore di accettare la cryptovaluta come metodo di pagamento per estinguere il debito pecuniario (salvo la convenzione di clausole cd. "effettivo" che riconoscono efficacia estintiva ad una particolare moneta in solutione): l'accettazione viene effettuata al valore nominale pieno della moneta sulla base del principio nominalistico. Il riconoscimento di questa facultas solutionis attraverso il pagamento in Bitcoin non esclude, tuttavia, la possibilità di impiego di altre valute accettate come aventi corso legale nello Stato (il dollaro, il Colon salvadoregno etc.).

Come ricordato, il provvedimento legislativo costituisce, allo stato attuale, una mera base programmatica, la cui effettività sarà da misurarsi attraverso i diversi atti e regolamenti che andranno a definire le misure attuative. Deve tuttavia registrarsi un primo importante arresto da parte della Banca Mondiale che, a fronte di una richiesta di assistenza formulata del governo salvadoregno nell'implementazione del progetto, ha comunicato il proprio dissenso rispetto all'operazione. In particolare, il rifiuto poggia sui dubbi espressi dalla Banca Mondiale circa la trasparenza del processo e la sostenibilità energetica del mining. Studi recenti (*Cambridge Bitcoin Electricity Consumption Index*, 2021) mostrano che l'estrazione di Bitcoin produce un impatto in termini di consumo annuale di energia elettrica superiore a quello dell'Argentina, data la potenza di calcolo elevatissima richiesta dai computer che effettuano attività di mining. Al rifiuto di cooperazione da parte della Banca Mondiale ha fatto poi eco l'avvertimento del Fondo Monetario Internazionale secondo cui l'adozione del Bitcoin come moneta a corso legale solleva una serie di questioni macroeconomiche, finanziarie e legali che richiedono un'analisi molto attenta, poiché le cryptovalute possono comportare rischi significativi se non vengono adottate misure normative efficaci.

https://www.diariooficial.gob.sv/diarios/do-2021/06-junio/09-06-2021.pdf

9. Il provvedimento del 22 luglio 2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders

Con provvedimento n. 285 del 22 luglio 2021 il Garante per la protezione dei dati personali (il "**Garante**") ha emesso un'ordinanza di ingiunzione nei confronti della società Deliveroo Italy S.r.l. ("**Deliveroo**"), con riferimento al trattamento dei dati personali dei ciclo fattorini, c.d. *riders* (il "**Provvedimento**").

Deliveroo - come è noto - è una società che svolge, per mezzo di una piattaforma digitale, un'attività di consegna di cibo ed altri beni, forniti da molteplici esercenti, avvalendosi di personale a ciò dedicato (i c.d. *riders*).

Sulla base degli elementi di fatto relativi al modello di organizzazione del lavoro (che avviene in maniera integralmente automatizzata attraverso una app che ogni *rider* deve scaricare sul proprio dispositivo mobile), riscontrati nella fase istruttoria, il Garante ha ritenuto il trattamento dei dati personali dei *riders* posto in essere da Deliveroo illegittimo per:

(i) violazione dei principi di liceità, correttezza, minimizzazione e limitazione della conservazione, in relazione all'art. 5 lett. a) c) ed e) del Regolamento UE 2016/679 ("**GDPR**");

(ii) violazione delle regole in materia di informativa (art. 13 GDPR) e di trattamenti automatizzati, con particolare riferimento all'obbligo di adottare delle misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato (art. 22, par.3 GDPR);

(iii) violazione delle regole in maniera di protezione dei dati sin dalla progettazione e per impostazione predefinita (*privacy by design* e *by default*, art. 25 GDPR);

(iv) violazione delle regole sulla tenuta del Registro dei trattamenti (art. 30, par.1, lett. c), f) e g) GDPR);

(v) mancata adozione delle misure di sicurezza nel trattamento dei dati (art. 32 GDPR);

(vi) violazione delle regole in materia di valutazione di impatto del trattamento (art.

35 GDPR), anche in considerazione delle tecnologie utilizzate;

(vii) mancata comunicazione - fino al 31 maggio 2019 - dei dati di contatto del responsabile della protezione dei dati all'Autorità di controllo (art. 37, par. 7 GDPR);

(viii) violazione delle regole in materia di trattamento dei dati personali nell'ambito dei rapporti di lavoro (art. 88 GDPR);

(ix) mancata adozione delle garanzie in materia di controllo a distanza (art. 114 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR, d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101).

In conseguenza di tale accertamento, il Garante ha, pertanto, ingiunto a Deliveroo, in base a quanto previsto dall' art. 58 par. 2 lett. d) GDPR, di:

(i) predisporre correttamente entro 60 giorni dal ricevimento del Provvedimento, i documenti in materia di informativa, fornendo precise indicazioni ai *riders* in merito al funzionamento del sistema di assegnazione degli ordini attualmente in uso (comprese le indicazioni sulla tipologia dei dati trattati e sui trattamenti dei dati già raccolti dal sistema di elaborazione delle statistiche), il registro dei trattamenti e la valutazione di impatto;

(ii) individuare correttamente, entro 60 giorni dal ricevimento del Provvedimento, i tempi di conservazione dei dati;

(iii) individuare entro 60 giorni dal ricevimento del Provvedimento, le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno con riferimento al diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, in relazione ai trattamenti automatizzati, compresa la profilazione, effettuati mediante la piattaforma;

(iv) individuare misure appropriate volte alla verifica periodica della correttezza ed accuratezza dei risultati dei sistemi algoritmici, anche al fine di garantire che sia minimizzato il rischio di errori e conformarsi a quanto stabilito dall'art. 47-quinquies, d. lgs. n. 81/2015 (come modificato dal Decreto legge 3 settembre 2019, n. 101, convertito con modificazioni in Legge 2 novembre 2019, n. 128 – recante norme specifiche a tutela del lavoro svolto mediante piattaforme digitali e, in particolare, dell'attività lavorativa dei c.d. *riders*) in materia di divieto di discriminazione, accesso alla piattaforma ed esclusione dalla piattaforma; detta attività dovrà essere avviata dalla Società entro 60 giorni dal ricevimento del Provvedimento e la verifica dovrà essere conclusa entro i successivi 90 giorni;

(v) individuare misure appropriate volte ad introdurre strumenti per evitare usi impropri e discriminatori dei meccanismi reputazionali basati su *feedback*, con obbligo di ripetere la verifica ad ogni modifica dell'algoritmo, relativamente all'utilizzo dei f*eedback* per il calcolo del punteggio; detta attività dovrà essere avviata dalla Società entro 60 giorni dal ricevimento del Provvedimento e la verifica dovrà essere conclusa entro i successivi 90 giorni;

(vi) applicare, entro 60 giorni dal ricevimento del Provvedimento, i principi di minimizzazione e di *privacy by design* e *by default*, in relazione al trattamento dei dati dei *riders*;

(vii) individuare i soggetti autorizzati ad accedere ai sistemi, in qualità di supervisori, con visibilità non limitata su base territoriale, definendo ipotesi predeterminate e specifiche finalità che rendano necessario tale accesso e adottando le misure appropriate per assicurare la verifica di tali accessi;

(viii) adempiere, entro 60 giorni dal ricevimento del Provvedimento, a quanto previsto dall'art. 4, comma 1, l. 20.5.1970, n. 300, con riferimento al divieto di controllo a distanza dei lavoratori.

Il Garante ha inoltre applicato ai danni ddi Deliveroo una sanzione pecuniaria di Euro 2.500.000.

ARIANNA NERI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9685994

10. Il pronunciamento del 28 maggio 2021 della Suprema Corte del Popolo della Repubblica Popolare Cinese sul valore probatorio dei dati registrati su blockchain

Il 28 maggio 2021, la Suprema Corte del Popolo della Repubblica Popolare Cinese ha pubblicato le *Regole sul Contenzioso Online dei Tribunali del Popolo* (人民法院在线诉讼规则, in seguito le 'Regole'). Le Regole, composte di 39 articoli ed entrate in vigore il 1° agosto 2021, illustrano i principi fondamentali, l'ambito d'applicazione e le condizioni per l'accesso ai contenziosi online e forniscono informazioni sulle fasi della procedura, la modalità di svolgimento delle udienze, la pubblicazione e l'esecuzione delle sentenze, l'archiviazione dei casi. Particolarmente innovativa, risulta la previsione della revisione dell'autenticità delle prove giudiziali presentate dalle parti mediante uso di tecnologia *blockchain*. Si prevede che le prove elettroniche presentate attraverso la tecnologia *blockchain* e tecnicamente verificate si presumeranno esenti da manomissioni dopo essere state caricate sulla catena, a meno che non vi siano prove contrarie sufficienti per ribaltare la presunzione (Articolo 16). Le Regole forniscono inoltre indicazioni su come rivedere l'autenticità delle prove elettroniche archiviate utilizzando la tecnologia *blockchain*, compreso come determinare se le prove elettroniche sono state alterate prima di essere archiviate sulla catena (Articoli 17-19). La Suprema Corte, nel comunicato ufficiale, ha affermato che le "prove *blockchain*" porteranno maggiore trasparenza, sicurezza, tracciabilità ed efficienza alle controversie online in Cina, dimostrando quindi di fare pieno affidamento su questa tecnologia.

CORRADO MORICONI

http://www.court.gov.cn/zixun-xiangqing-309551.html
http://english.court.gov.cn/2021-06/18/content_37545136.htm