21

Il Garante ha continuato a coordinare il sottogruppo "*Financial matters*" che nell'ambito del Comitato è incaricato di approfondire le diverse questioni legate all'applicazione della disciplina sulla protezione dei dati nel settore finanziario.

PSD2 e RGPD

Una delle questioni che ha maggiormente impegnato il sottogruppo è stato il rapporto tra il RGPD e la direttiva (UE) 2015/2366 sui servizi di pagamento (cd. PSD2), due normative chiave della legislazione europea degli ultimi anni. La direttiva PSD2 presenta novità importanti nel sistema dei pagamenti consentendo a nuovi soggetti di attuare servizi che un tempo erano prerogativa pressoché esclusiva delle banche, consentendo ad essi di accedere ad una mole considerevole di dati finanziari non solo dei clienti, ma anche di soggetti terzi, ad esempio dei beneficiari di ordini di pagamenti. Il Comitato, che si era già occupato di alcune questioni legate alla PSD2 con la risposta a una lettera dell'europarlamentare Sophie in't Veld, fornendo prime indicazioni su alcuni punti controversi del rapporto tra tale direttiva e RGPD, ha ritenuto necessario avviare una riflessione più approfondita sul tema anche alla luce degli esiti di un *workshop*, organizzato dal segretariato e tenutosi a Bruxelles il 27 febbraio 2019, nel corso del quale i diversi *stakeholders* si sono confrontati sulle parti più complesse dell'interazione tra PSD2 e RGPD, in particolare sull'individuazione della corretta base giuridica per il trattamento dei dati relativi ai terzi effettuato dai nuovi operatori nei servizi di pagamento e delle deroghe al divieto di trattare speciali categorie di dati ai sensi dell'art. 9 del RGPD da essi utilizzabili.

Scambi di informazioni tra autorità di controllo dei mercati finanziari ai fini di cooperazione

È stato concluso il lavoro del Comitato sullo scambio di informazioni tra autorità di controllo dei mercati finanziari nell'ambito della loro attività di cooperazione. In tale attività di scambio occorre che i trasferimenti di dati dalle autorità finanziarie europee alle loro omologhe extra-UE siano effettuati nel rispetto dei principi di protezione dati. In particolare, in base all'art. 46, par. 3, lett. *b*), del RGPD, le autorità pubbliche o organismi pubblici possono stipulare accordi amministrativi, che includano diritti effettivi e azionabili per gli interessati, per assicurare le garanzie necessarie a legittimare i trasferimenti di dati verso Paesi sforniti di adeguatezza. Come anticipato (cfr. par. 4.8), il Comitato ha esaminato il modello di accordo di cui potranno avvalersi le autorità finanziarie per i trasferimenti dei dati extraeuropei predisposto da Esma unitamente a Iosco. Con il parere 4/2019 adottato il 12 febbraio 2019 (ai sensi dell'art 64, par. 2, del RGPD) il Cepd ha concluso che la versione finale di tale accordo assicura le garanzie adeguate necessarie a trasferire i dati, ed ha comunque fornito alcune ulteriori indicazioni riguardo all'implementazione dei meccanismi di tutela posti in essere dall'accordo stesso.

FATCA

In ambito finanziario è altresì proseguita l'attività del Comitato relativa all'analisi delle implicazioni della normativa statunitense FATCA (*Foreign Account Tax Compliance Act*) sulla tutela della vita privata e sul principio di non discriminazione, previsti dagli artt. 8 e 14 della CEDU. L'8 febbraio 2019 il Comitato ha adottato una dichiarazione (*Statement* 1/2019) in risposta alla risoluzione del 5 luglio 2019 del Parlamento europeo e alle richieste dell'associazione dei cd. *Accidental Americans*, che hanno sollecitato un intervento del Comitato sulle implicazioni di FATCA. La dichiarazione, richiamando i diversi interventi dell'allora Gruppo Art. 29 sul tema, annuncia l'avvio da parte del Comitato della predisposizione di linee guida sugli strumenti per il trasferimento dei dati ai sensi dell'art. 46 del RGPD, che offriranno indicazioni anche per il caso FATCA, in particolare con riferimento alla garanzie minime che dovranno essere inserite, per i trasferimenti di dati all'estero, negli strumenti giuridicamente vincolanti tra autorità pubbliche ai sensi dell'art. 46, par. 2, lett. *a*), del RGPD o negli accordi amministrativi tra le stesse ai sensi dell'art. 46, par. 3, lett. *b*), del RGPD. Tali linee guida costituiranno uno strumento utile anche

21

ai fini della valutazione degli accordi intergovernativi firmati tra gli Stati membri e il governo statunitense per far sì che l'applicazione di FATCA sia conforme ai principi di protezione dati previsti dal RGPD.

È stata inoltre avviata la discussione sulla base giuridica della conservazione dei dati relativi a carte di credito, effettuata dalle piattaforme di *e-commerce*, al fine di facilitare gli acquisti successivi da parte dei loro clienti, nonché sul tema delle criptovalute nell'ambito della più ampia riflessione in materia di *blockchain* avviata dagli specifici sottogruppi cui il Comitato ha dato mandato.

Il tema delle criptovalute è stato altresì discusso dal Comitato con riferimento all'iniziativa lanciata da Facebook in collaborazione con l'associazione svizzera "Libra" sulla creazione di una nuova criptovaluta. La questione è stata già oggetto di una dichiarazione congiunta di diverse autorità per la protezione dei dati (di Albania, Australia, Burkina Fasu, Canada, Regno Unito, insieme all'EDPS e alla *Federal Trade Commission*) e di una lettera del *Commissioner* svizzero rivolta alla Presidente del Comitato affinché sia aperto un dialogo sui profili di protezione dei dati implicati in tale iniziativa.

Protezione dei dati e *law enforcement*

Il Comitato ha proseguito la sua attività relativa alla protezione dei dati nell'ambito delle attività di indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, oggetto della direttiva (UE) 2016/680.

CLOUD Act

È stata adottata la risposta congiunta del Comitato e del GCPD del 10 luglio 2019 sull'impatto della normativa statunitense "*CLOUD Act*" – che prevede la possibilità per le autorità statunitensi di richiedere ai fornitori di servizi i dati detenuti anche nel caso in cui siano conservati sul territorio extra-USA – sull'ordinamento UE. La lettera sottolinea che un accordo UE-USA riguardo all'accesso transfrontaliero dei dati che contenga efficaci garanzie a tutela dei diritti della persona rappresenta lo strumento più appropriato per assicurare un livello di protezione adeguato e la certezza giuridica per le imprese.

Sistemi ETIAS e ECRIS-TCN

È stata adottata la lettera del 13 novembre 2019 di risposta alla LIBE che nell'aprile 2019 aveva chiesto al Comitato di valutare due proposte di regolamento presentate dalla Commissione europea nel gennaio 2019 al fine di introdurre le modifiche tecniche necessarie a rendere pienamente operativo il sistema ETIAS e quello ECRIS-TCN, modificando gli atti giuridici riguardanti i sistemi informatici dell'UE (quali SIS, VIS, Eurodac, ecc.). Nella lettera adottata dal Comitato si chiarisce che i documenti in questione contengono in realtà solo modifiche volte a rendere applicabile il nuovo quadro per l'interoperabilità dei sistemi informativi sul quale il Gruppo Art. 29 aveva già manifestato grosse perplessità con il parere WP 266 dell'aprile 2018 e si sottolinea che le modifiche introdotte a sistemi informativi non ancora realizzati rischiano di ledere la trasparenza, il principio per cui i trattamenti devono essere fondati su regole chiare e certe nonché quelli di *privacy by design* e *by default*. La lettera ribadisce infine che il previsto sistema di interoperabilità solleva seri dubbi circa il rispetto del principio di finalità e dei diritti degli interessati.

Il secondo Protocollo addizionale alla Convenzione di Budapest

Il Comitato ha inoltre fornito il proprio contributo alla consultazione pubblica lanciata dal Comitato *cybercrime* (T-CY) del Consiglio d'Europa sulla bozza di secondo Protocollo addizionale alla Convenzione di Budapest, in particolare sui temi della cd. *direct disclosure*, ovvero la procedura che permette una diretta cooperazione tra le autorità di una Parte e un fornitore di servizi di comunicazione elettronica situato nel territorio di un'altra Parte al fine di ottenere informazioni relative al *subscriber*, e della procedura che permette ad una Parte di dare mandato ad un'altra al fine di obbligare un fornitore di servizi situato nel territorio di quest'ultima a esibire specifiche informazioni sul *subscriber* e i dati di traffico ad esso relativi. Il contributo del Cepd richiama le posizioni già assunte dal Gruppo Art. 29, dal Comitato

medesimo e dal Gepd in materia; sottolinea la necessità che la protezione dei dati sia inclusa nelle norme del Protocollo, rendendo l'accessibilità dei dati pienamente compatibile con i trattati UE e la CDFUE; ricorda che il Comitato rimane a disposizione per ulteriori contributi ai fini della preparazione delle specifiche previsioni normative in materia di protezione dati su cui il T-CY sta lavorando, auspicando il coinvolgimento tempestivo delle autorità di protezione dati nel processo di elaborazione del Protocollo. Con riferimento a specifiche previsioni normative in materia di protezione dei dati, il contributo sottolinea la necessità che il testo sia arricchito da tali previsioni, che riflettono i principi cardine UE ma anche quelli previsti dalla Convenzione 108+; richiama a tal proposito i principi sostanziali e procedurali che devono regolare l'accesso ai dati da parte delle autorità di *law enforcement* (accesso previsto da una chiara base legale; accesso individuale solo in relazione a individui sospettati di voler commettere o di aver commesso crimini gravi; autorizzazione da parte di autorità giurisdizionali; proporzionalità e qualità dei dati raccolti; speciali garanzie per dati sensibili; informativa agli interessati non appena possibile anche al fine di consentire l'esercizio dei propri diritti); sottolinea la necessità che agli interessati siano assicurati strumenti di tutela adeguati quantomeno equivalenti a quelli esistenti nel proprio stato; ricorda la necessità di inserire specifiche garanzie sui trasferimenti ulteriori, compreso il divieto di trasferire i dati verso paesi privi di un livello di protezione appropriato.

PNR

Il 9 ottobre 2019, il Comitato ha inoltre adottato una lettera di risposta alla parlamentare europea Sophie in't Veld, che aveva chiesto quale fosse la posizione dello stesso in merito al nuovo Accordo sul PNR (*Passenger Name Record*) oggetto della negoziazione tra la Commissione europea e il Canada. La nota di risposta richiama le posizioni già espresse dal Gruppo Art. 29 subito dopo il parere 1/2017 della Corte di giustizia sulla prima bozza di Accordo, in particolare sulla necessità che, in linea con gli orientamenti della Corte, gli accordi PNR rispettino pienamente i principi della CDFUE e anticipa l'intenzione di predisporre un proprio parere sulla nuova bozza di accordo non appena disponibile.

Commissione di controllo coordinato

Dopo la plenaria del Comitato del 3 dicembre 2019, si è svolto il primo incontro della Commissione di controllo coordinato sul trattamento dei dati svolto nell'ambito dei grandi sistemi informativi dell'UE che rafforzerà la cooperazione tra le diverse autorità di protezione dei dati in tale settore e garantirà verifiche più efficaci. La Commissione, istituita nell'ambito del Comitato e che riunisce le autorità europee di protezione dei dati, l'EDPS e le autorità di controllo degli Stati extra-UE che partecipano al sistema Schengen, si occuperà di vigilare sui sistemi informativi e sugli organismi, gli uffici e le agenzie operanti nei settori delle frontiere, dell'asilo e della migrazione (SIS, EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI). Nel corso della sua prima riunione, la Commissione ha eletto il Segretario generale del Garante Giuseppe Busia quale coordinatore e Iris Gnedler dell'Autorità federale tedesca in qualità di vice-coordinatore, per un mandato di due anni, ed ha altresì adottato il proprio regolamento interno.

Protezione dei dati e nuove tecnologie

In materia di nuove tecnologie e protezione dei dati, il tema dominante del 2019 è stato quello della possibile revisione della direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (cd. direttiva *e-Privacy*). Incessanti sono state infatti le discussioni, specie in seno al Consiglio dell'Unione, al fine di pervenire ad un testo condiviso da portare al trilogo con il Parlamento. Il Comitato è intervenuto sul tema adottando, il 13 marzo 2019, la Dichiarazione 3/2019 sul regolamento *e-Privacy* (*Statement* 3/2019), con la quale ha invitato gli Stati membri a finalizzare le proprie posizioni

21

Direttiva *e-Privacy* e RGPD

sulla proposta di regolamento *e-Privacy*, la cui adozione completerebbe il quadro europeo per la protezione dei dati fornendo ulteriori forti salvaguardie per tutti i tipi di comunicazioni elettroniche. Il Comitato ha invitato il legislatore dell'Unione a garantire che il futuro regolamento *e-Privacy* non fornisca una protezione inferiore a quella assicurata nell'attuale direttiva *e-Privacy*.

Su questo stesso tema, il Comitato ha adottato il 12 marzo 2019 il parere 5/2019 relativo all'interazione tra la direttiva UE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva *e-Privacy*) e il RGPD. Il parere – adottato a seguito di una richiesta avanzata, ai sensi dell'art. 64, par. 2, del RGPD, dall'Autorità belga di protezione dei dati – ha il fine di chiarire le competenze delle autorità di protezione dei dati nazionali allorché un trattamento di dati ricada sia sotto l'ambito applicativo del RGPD sia sotto quello della direttiva *e-Privacy*. L'Autorità belga aveva richiesto al Comitato chiarimenti in merito a, da un lato, competenza, compiti e poteri delle autorità di controllo per la protezione dei dati personali e, dall'altro, applicabilità dei meccanismi di cooperazione e coerenza del RGPD nei casi in cui al trattamento dei dati personali si applichi sia il RGPD che la direttiva *e-Privacy*.

In primo luogo, il parere rileva che vi sono molti esempi di attività di trattamento dei dati che rientrano nell'ambito di applicazione materiale sia della direttiva *e-Privacy* che del RGPD, come confermato anche dalla giurisprudenza della CGUE, ad esempio per l'uso di *cookie*. Il parere ribadisce che la direttiva *e-Privacy* prevede "norme speciali" in merito al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Tra queste figurano le disposizioni dell'art. 5, par. 3 che richiedono il consenso dell'utente per conservare informazioni, compresi i dati personali, nel dispositivo dell'utente finale o per avere accesso a tali informazioni (ad es, tramite *cookie*) e l'art. 6, che limita esplicitamente le condizioni alle quali possono essere trattati i dati relativi al traffico, compresi i dati personali degli abbonati e degli utenti di un servizio di comunicazione elettronica accessibile al pubblico. Conformemente al principio della *lex specialis derogat legi generali*, queste disposizioni specifiche in materia di *e-Privacy* hanno la precedenza sulle disposizioni (più generali) del RGPD (come l'art. 6 del RGPD, che individua le basi giuridiche possibili per il trattamento dei dati personali). In tutti gli altri casi in cui il trattamento dei dati personali non è specificamente disciplinato dalla direttiva *e-Privacy* (o per cui la direttiva *e-Privacy* non prevede una "norma speciale"), si applica il RGPD. Ad esempio, si applicheranno le disposizioni del RGPD relative all'esercizio dei diritti degli interessati in relazione ai loro dati personali, in quanto non previste delle disposizioni specifiche nella direttiva *e-Privacy*. Analogamente, qualsiasi successivo trattamento di dati personali (come i dati personali ottenuti tramite i *cookie*) deve fondarsi su una delle basi giuridiche ai sensi dell'art. 6 del RGPD per essere lecito e rispettare tutte le altre disposizioni del RGPD.

Quanto alla competenza delle autorità, il parere precisa che qualora il trattamento dei dati personali rientri nell'ambito di applicazione materiale sia del RGPD sia della direttiva *e-Privacy*, le autorità sono competenti a vigilare sulle operazioni di trattamento dei dati che sono disciplinate dalle norme nazionali in attuazione della direttiva *e-Privacy* solo se la legislazione nazionale conferisce loro tale competenza. Inoltre, tale controllo deve avvenire attraverso i poteri di vigilanza attribuiti all'autorità di protezione dei dati dalla legislazione nazionale che attua la direttiva *e-Privacy*. La competenza delle autorità ai sensi del RGPD rimane intatta per quanto riguarda le operazioni di trattamento dei dati non soggette a norme speciali contenute nella direttiva *e-Privacy*. Il semplice fatto che una parte del trattamento rientri anche nel campo di applicazione della direttiva *e-Privacy* non limita infatti

la competenza delle autorità di controllo ai sensi del RGPD. Nell'esercizio dei loro compiti e poteri ai sensi del RGPD, le autorità di protezione dei dati possono tener conto delle disposizioni della direttiva *e-Privacy* solo se: una violazione del RGPD costituisce anche una violazione delle disposizioni nazionali di attuazione della direttiva *e-Privacy*. La decisione dell'autorità per la protezione dei dati dovrà tuttavia essere giustificata sulla base del RGPD se la suddetta autorità non è competente, in base al diritto nazionale, ad applicare direttamente le disposizioni nazionali di attuazione della direttiva *e-Privacy*.

Quanto ai meccanismi di cooperazione e coerenza a disposizione delle autorità nell'ambito del RGPD, il parere prevede che gli stessi non si applicano per l'attuazione nazionale della direttiva *e-Privacy*. Tuttavia, i meccanismi di cooperazione e coerenza restano pienamente applicabili ai trattamenti soggetti alle disposizioni generali del RGPD (e non a una "norma speciale" contenuta nella direttiva *e-Privacy*).

Net Neutrality

In vista della revisione delle proprie linee guida in materia di *Net Neutrality*, l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC - *Body of European Regulators for Electronic Communications*) ha inviato al Comitato alcune domande in tema di protezione dei dati sia con riferimento al RGPD che alla direttiva *e-Privacy,* in particolare in relazione alla gestione dei dati di traffico e della fatturazione (offerte a cd. *zero-rating*). La nota di risposta, datata 3 dicembre 2019, richiama l'attenzione sul rispetto del principio di necessità e proporzionalità: i dati trattati per le finalità sopra richiamate devono essere quelli strettamente necessari al loro perseguimento (ovvero il loro trattamento deve essere "*required, unconditional and without alternative*") e i *service provider* devono essere in grado di dimostrare il rispetto di questi principi ogniqualvolta trattano i dati a tale scopo. A parere del Comitato, i dati relativi agli indirizzi URL e ai nomi di dominio possono essere trattati per finalità di fatturazione solo con il consenso dell'interessato. La lettera invita gli *Internet service provider* a utilizzare sistemi di gestione del traffico meno invasivi evitando la *"deep inspection*" dei pacchetti, indicando due possibili esempi (*Explicit Congestion Notification* - ECN o *Differentiated Services Code Point* - DSCP).

Linee guida sulla videosorveglianza

Alla luce delle novità tecnologiche che negli ultimi anni hanno caratterizzato l'ambito della videosorveglianza, il Comitato ha adottato, il 10 luglio 2019, le nuove linee guida sulla videosorveglianza (linee guida 3/2019) che chiariscono in quali termini il RGPD si applichi al trattamento dei dati personali quando si utilizzano dispositivi video e che mirano a garantirne un'applicazione coerente.

Le linee guida, modificate a gennaio 2020 all'esito della procedura di consultazione pubblica, riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti per finalità strettamente personali e la divulgazione di filmati a terzi.

Le linee guida ribadiscono che, nell'utilizzare i sistemi di videosorveglianza, devono prioritariamente essere rispettati i principi sanciti dall'art. 5 del RGPD applicabili al trattamento di dati personali, tra i quali i principi della liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati. Prima dell'installazione, è necessario accertare che lo strumento sia proporzionato alla finalità perseguita. Il Comitato considera la videosorveglianza come una *extrema ratio* consentendone l'utilizzo solamente quando gli scopi perseguiti non possono essere raggiunti con altre modalità meno invasive. Per minimizzare la raccolta dei dati, il

21

Comitato suggerisce di ricorrere a soluzioni di cancellazione automatica mediante sovrascrittura del registrato, con video accessibili solo in caso di necessità e, quali misure necessarie alla corretta gestione e alla raccolta dei dati personali provenienti da sistemi di videosorveglianza, individua le seguenti: redazione di una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35, par. 3, lett. *c*), del RGPD, in tutti i casi in cui vi sia una sorveglianza sistematica su larga scala di una zona accessibile al pubblico; designazione di un Rpd nei casi in cui vi sia un monitoraggio regolare e sistematico degli interessati su larga scala, ai sensi dell'art. 37, par. 1, lett. *b*), del RGPD.

Linee guida in materia di protezione dei dati *by design* e *by default*

Sempre in tema di nuove tecnologie, il Comitato ha adottato il 13 novembre 2019 le linee guida 4/2019 in materia di *data protection by design* e *by default* nel testo sottoposto a consultazione pubblica, il cui termine è scaduto il 16 gennaio 2020.

Il documento si concentra sugli obblighi fissati in materia dall'art. 25 del RGPD. L'obbligo fondamentale in questo caso è l'attuazione efficace dei principi in materia di protezione dei dati e dei diritti nonchè delle libertà degli interessati fin dalla progettazione e per impostazione predefinita. Ciò richiede che i titolari del trattamento mettano in atto adeguate misure tecniche e organizzative volte ad assicurare l'efficace implementazione dei principi di protezione dei dati. Le linee guida sviluppano questi temi e il Comitato sottolinea più volte che la *data protection by design* e *by default* (DPbDD) è un requisito fondamentale che tutti i titolari devono soddisfare, anche quelli di piccole dimensioni, così come disciplinato dall'art. 25 del RGPD, tenendo conto di una molteplicità di fattori (alcuni dei quali menzionati dal Regolamento stesso). Sia al tempo in cui si determinano i mezzi del trattamento (progettazione del trattamento) e sia all'atto del trattamento stesso, il titolare deve adottare le adeguate misure tecniche ed organizzative per soddisfare i requisiti del RGPD e tutelare i diritti degli interessati.

Il Comitato chiarisce anche il significato di DPbDD dal punto di vista pratico: le linee guida elencano "*design and default elements*" per attuare efficacemente i principi di protezione dei dati facendo ricorso ad esempi; inoltre, esse entrano nel merito dei meccanismi di certificazione menzionati dall'art. 25, par. 3, del RGPD, chiarendo che gli organismi di certificazione dovranno valutare il processo di progettazione (cioè, il processo di determinazione dei mezzi di trattamento), la *governance* e le misure organizzative nonché le misure di garanzia, il tutto nel contesto del trattamento. Il Comitato ribadisce che le autorità di controllo valuteranno la presenza di tali certificazioni ma non ne saranno vincolate (art. 42, par. 4). Infine, nel responsabilizzare non solo il titolare ma anche i responsabili del trattamento ed i *technology providers*, rammentando che tali operatori rivestono un ruolo chiave in vista della DPbDD, il Comitato fornisce 11 raccomandazioni su come i titolari e i responsabili del trattamento nonché i fornitori di tecnologia possano cooperare per raggiungere gli obiettivi di DPbDD.

Linee guida sui criteri relativi al diritto all'oblio

In data 2 dicembre 2019 sono state adottate dal Comitato linee guida sui criteri per l'esercizio del diritto all'oblio relativo ai motori di ricerca (linee guida 5/2019), poste in consultazione pubblica fino al 5 febbraio 2020. Loro obiettivo è quello di fornire una corretta interpretazione del diritto all'oblio (art. 17 del RGPD) nei casi di richiesta di de-indicizzazione (cd. *delisting*) da parte degli interessati che rivolgono l'istanza ai motori di ricerca, alla luce di quanto statuito dalla CGUE all'esito del noto caso C-131/12 (Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González, sentenza del 13 maggio 2014) e sono state adottate alla luce dei numerosi reclami pervenuti alle autorità di controllo in relazione al rifiuto da parte dei fornitori dei motori di ricerca di aderire a molte delle richieste di cancellazione ricevute.

21

Le linee guida si compongono di due parti: la prima si sofferma sui presupposti che inducono l'interessato ad effettuare una richiesta di deindicizzazione; la seconda, invece, si sofferma sul regime di eccezioni, che consentono al titolare del trattamento di non adempiere alla richiesta dell'interessato.

L'art. 17 del RGPD riconosce all'interessato il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, se sussiste almeno uno dei sei motivi elencati dalla lett. *a*) alla lett. *f*) del suo par. 1. Nel soffermarsi su ciascuno di tali motivi, il Comitato stabilisce che nel primo caso, ossia quando i dati personali non sono più necessari in relazione alle finalità per le quali sono stati raccolti o altrimenti trattati, nell'analizzare le richieste di *delisting* e al fine di contemperare il diritto alla protezione dei dati con il diritto degli utenti di internet ad accedere alle informazioni, le autorità nazionali devono valutare se, nel corso del tempo, i dati personali sono diventati obsoleti o non sono stati aggiornati, in relazione alle finalità del trattamento originario e ai connessi periodi di conservazione. In merito al secondo motivo – l'interessato ha revocato il consenso su cui si basa il trattamento – le linee guida chiariscono che tale disposizione non si applica ai gestori del motore di ricerca, atteso che il consenso è stato fornito dall'interessato non a tali operatori, ma, ove necessario, ai titolari delle pagine web indicizzate. Pertanto, nel caso in cui l'interessato revochi il proprio consenso all'uso dei dati che lo riguardano su una determinata pagina web, sarà il titolare di quest'ultima a dover richiedere la de-indicizzazione ai motori di ricerca.

In ogni caso, l'istante potrà ottenere la cancellazione dei dati personali, opponendosi al trattamento (terzo caso), purché non vi siano motivi legittimi prevalenti sugli interessi, i diritti e le libertà del richiedente, motivi la cui sussistenza, peraltro, dovrà essere provata dal *provider* del motore di ricerca. Se, quindi, un risultato di ricerca reca un pregiudizio all'interessato quando fa domanda per un lavoro o mina la sua reputazione, il fornitore dovrà considerare il diritto all'informazione, il ruolo pubblico dell'istante, il legame tra le informazioni indicizzate e la vita professionale del medesimo, la circostanza che le informazioni costituiscano incitamento all'odio o configurino un reato (es. diffamazione, calunnia) o che, infine, siano risalenti nel tempo.

Con riferimento al quarto motivo – i dati personali sono stati trattati illecitamente –, secondo il Comitato, l'illiceità deve essere interpretata in senso lato, avendo riguardo non solo alle norme del RGPD, ma anche alle leggi nazionali o alle decisioni giudiziarie di ciascuno Stato membro.

Rispetto al quinto motivo – la richiesta di cancellazione è basata su un obbligo legale previsto dalla normativa nazionale o europea o da un provvedimento dell'autorità giurisdizionale –, la richiesta di cancellazione ha una base normativa specifica e quindi non dovrebbero porsi problemi applicativi o interpretativi di rilievo.

Circa il sesto motivo – i dati personali di cui si richiede la cancellazione sono stati raccolti in relazione all'offerta di servizi della società dell'informazione resi a un minore –, le linee guida precisano che le attività dei gestori di motori di ricerca potrebbero rientrare tra i servizi della società dell'informazione e pertanto si dovrebbero eliminare i contenuti relativi ai minori.

Dopo aver analizzato le ipotesi in cui è possibile esercitare il diritto all'oblio, le linee guida affrontano i casi in cui la richiesta di eliminazione non può essere accolta, in base all'art. 17 del RGPD. Quest'ultimo non si applica, *in primis*, quando il trattamento dei dati personali è necessario per l'esercizio del diritto alla libertà di espressione, incluso il libero accesso alle informazioni. Il Comitato richiama quanto specificato dalla CGUE sul bilanciamento tra diritto all'informazione e diritto alla protezione dei dati, ovvero che l'equilibrio tra tali interessi contrapposti dipende,

in particolare, dal ruolo svolto dall'interessato nella vita pubblica, nonché dal preponderante interesse del grande pubblico ad avere accesso alle informazioni oggetto della richiesta di cancellazione. Altro motivo per cui non si applica l'art. 17 è l'esistenza di disposizioni di legge che obblighino a non cancellare i dati personali. Sul punto, le linee guida ritengono sia improbabile che i fornitori dei motori di ricerca siano obbligati per legge a diffondere determinate informazioni e ciò in quanto essi non creano informazioni. Non viene tuttavia esclusa la possibilità che la legge di uno Stato membro possa imporre tale obbligo ai *provider*, stabilendo, peraltro, un limite di tempo alla pubblicazione, superato il quale, l'esenzione non è più applicabile e la richiesta di *delisting* può essere accolta.

Al di là di tale possibilità, il Comitato afferma che l'esistenza di un obbligo legale di pubblicazione imposto ai titolari dei siti web sorgente non implica necessariamente che il fornitore del motore di ricerca debba rigettare la richiesta di cancellazione. Il diritto di cui all'art. 17 del RGPD è escluso invece nel caso in cui il trattamento avvenga in esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di un pubblico potere. Il Comitato precisa che i fornitori di motori di ricerca, non essendo autorità pubbliche, non esercitano poteri pubblici ed è altresì improbabile che le leggi degli Stati membri possano stabilire diversamente, ovvero che la loro attività o parte di essa sia necessaria per il raggiungimento di un interesse pubblico.

Quanto alle finalità di archiviazione nell'interesse pubblico, della ricerca scientifica o storica o per scopi statistici che legittimerebbero il rigetto della richiesta di *delisting*, in base alle linee guida il fornitore del motore di ricerca deve essere in grado di dimostrare che la cancellazione di un determinato contenuto della pagina dei risultati rappresenta un grave ostacolo o impedisce il raggiungimento delle citate finalità, le quali, secondo il Comitato, possono tra l'altro essere perseguite obiettivamente dal *provider*, senza che sia necessario un collegamento tra il nome dell'interessato e i risultati della ricerca.

Dichiarazione 2/2019 sull'uso di dati personali nel corso di campagne politiche

Il Comitato ha adottato il 13 marzo 2019 la Dichiarazione 2/2019 sull'uso di dati personali nel corso di campagne politiche. In vista delle elezioni europee e di altre elezioni svoltesi in diversi Stati membri nel 2019 (e oltre), il Comitato ha richiamato l'attenzione sull'uso dei dati personali durante le campagne elettorali. Ad avviso del Comitato, le tecniche di trattamento dei dati a fini politici possono comportare gravi rischi, non solo in relazione alla *privacy* e alla protezione dei dati, ma anche rispetto all'integrità del processo democratico. Nel proprio *statement*, il Comitato ha così evidenziato una serie di punti chiave che devono essere presi in considerazione quando i partiti politici elaborano i dati personali nel corso delle attività elettorali.

Protezione dei dati e *e-Health*

In materia di *e-Health* è proseguito il lavoro del Comitato sul tema del trattamento dei dati dei pazienti nell'ambito dell'*e-Health Network*, la rete volontaria di collegamento delle autorità nazionali responsabili dell'assistenza sanitaria *online* degli Stati membri prevista dall'art. 14 della direttiva 2011/24/UE sull'assistenza sanitaria transfrontaliera (cfr. anche Relazione 2018, p. 194).

A seguito di una richiesta di consultazione da parte della Commissione, avanzata ai sensi dell'art. 42, par. 2, del regolamento (UE) 2018/1725 e dell'art. 70, par. 1, del RGPD, in merito alla revisione della decisione di esecuzione della Commissione 2011/890/EU che disciplina l'*e-Health Network*, il Comitato e il GCPD hanno adottato il primo parere congiunto (1/2019) volto a fornire alcune indicazioni sugli aspetti relativi alla protezione dei dati personali riguardanti il trattamento delle informazioni sui pazienti (prescrizioni elettroniche e *patient summary*) posto in essere dall'infrastruttura dei servizi digitali per l'*e-Health* (eHDSI) messa a disposi-

zione dalla Commissione (si tratta di una rete IT privata denominata TESTA che consente lo scambio dei dati sanitari elettronici tra i punti di contatto nazionali per l'*e-Health* dei 22 Stati membri partecipanti e facilita l'interoperabilità dei sistemi europei di sanità elettronica). Il Comitato ha fornito indicazioni circa il possibile ruolo di responsabile della Commissione in relazione al trattamento dei dati personali dei pazienti attraverso la messa a disposizione dell'eHDSI e ha richiamato l'attenzione della stessa sulla necessità di introdurre l'elenco degli obblighi del responsabile, ai sensi dell'art. 28, par. 8, del RGPD, nella revisione della decisione di esecuzione n. 2011/890/UE del 22 dicembre 2011 che stabilisce le norme per l'istituzione, la gestione e il funzionamento dell'*e-Health network*.

Sperimentazione clinica e RGPD

A seguito di una richiesta di consultazione indirizzata al Comitato dalla Commissione europea (DG SANTE) su alcune FAQ che la stessa intendeva predisporre in ordine al rapporto tra il RGPD e il regolamento (UE) n. 536/2014 sulla sperimentazione clinica di medicinali per uso umano, il Comitato ha reso, ai sensi dell'art. 70, par. 1, lett. *b*), del RGPD, un parere relativo all'interazione tra i due regolamenti (parere 3/2019).

Il documento si sofferma sulle differenti basi giuridiche per il trattamento dei dati nel contesto delle sperimentazioni cliniche e dei trattamenti ulteriori, per finalità di ricerca, dei dati raccolti nel corso delle stesse. Il Comitato ricorda che le basi giuridiche possono essere differenti a seconda delle finalità cui sono preordinate le diverse operazioni di trattamento e che il consenso informato, richiesto per la partecipazione allo studio clinico dal regolamento sulle sperimentazioni, è essenzialmente una misura per garantire la dignità e l'integrità delle persone che partecipano allo studio in conformità alla dichiarazione di Helsinki e non la base giuridica del trattamento dei dati.

Processo di revisione del Codice mondiale Anti-doping

Il Gruppo di lavoro sugli sport del Consiglio dell'UE si è rivolto al Comitato per chiedere una valutazione sulla compatibilità con il quadro UE del progetto di Codice mondiale Anti-doping per il 2021 e dei relativi "*International Standard*", con particolare riferimento a quello riguardante la protezione dei dati e alla tutela della *privacy* (ISPPPI).

La lettera di risposta del Comitato, datata 9 ottobre 2019, nel prendere atto dei miglioramenti apportati dall'Agenzia mondiale Anti-doping (WADA) a tali regole nel corso delle precedenti revisioni delle stesse, in linea con le indicazioni fornite a suo tempo dal Gruppo Art. 29 (cfr. i pareri del Gruppo Art. 29 4/2009 - WP 162 e 3/2008 - WP156 nonché la lettera del 5 marzo 2013, Ref. Ares (2013)289160), si focalizza su alcune questioni (molte delle quali già evidenziate dallo stesso Gruppo) che sollevano qualche criticità specie alla luce del nuovo quadro giuridico introdotto dal RGPD e fornisce alcune indicazioni al riguardo. In particolare, il Comitato si sofferma sulla possibilità di estendere l'applicazione delle regole Anti-doping ad atleti che svolgono attività sportiva ricreativa, considerandola un'interferenza sproporzionata nel diritto alla *privacy* e alla protezione dei dati degli atleti; sulla liceità del trattamento dei dati personali, rispetto alla quale si ribadisce che il consenso dell'atleta non può essere considerato una valida base giuridica; sulla vincolatività dello standard internazionale sulla protezione dei dati rispetto alle previsioni dello stesso Codice mondiale Anti-doping o di eventuali altre norme applicabili che forniscano un livello inferiore di protezione; sui periodi di conservazione dei dati e dei campioni biologici degli atleti, ritenuti in alcuni casi non proporzionati; sugli obblighi di pubblicazione in Internet delle violazioni delle regole Anti-doping, rilevandone il carattere automatico e indiscriminato.

21

21.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

Europol Cooperation Board

In virtù del nuovo quadro normativo creato dal regolamento (UE) 2016/794, entrato in vigore il 1° maggio 2017, la supervisione sull'attività svolta dall'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) è svolta dal Gepd. Rimane di competenza delle autorità nazionali di protezione dei dati, il controllo sulla legittimità della comunicazione di dati ad Europol da parte delle Forze di polizia e la verifica circa il rispetto dei diritti degli interessati. Al fine di assicurare una stretta cooperazione tra il Gepd e le autorità nazionali è stato istituito, con funzioni consultive, un Consiglio di cooperazione (*Europol Cooperation Board*) che si è riunito, nel 2019, l'8 maggio e il 28 novembre. Nel corso di queste riunioni sono state condivise le informazioni sulle attività di vigilanza su Europol, ivi comprese quelle sui principali risultati delle ispezioni svolte, sul numero crescente di dati inviati a Europol dagli Stati membri, sul trattamento dei dati su indagati di età inferiore ai 18 anni, sulle conseguenze della Brexit e su FIU.net (una rete informatica che supporta le unità di informazione finanziaria nell'UE nella loro lotta contro il riciclaggio di denaro e il finanziamento del terrorismo).

Gruppo di coordinamento della supervisione del Sistema d'informazione Schengen (SIS II)

Il sistema d'informazione Schengen (SIS II) è il sistema d'informazione centralizzato su larga scala che viene utilizzato come strumento d'ausilio per i controlli sulle persone e sugli oggetti alle frontiere esterne dello spazio Schengen. Secondo quanto previsto dal quadro giuridico del SIS II (regolamento CE 1987/2006 e decisione del Consiglio 2007/533/GAI), la supervisione coordinata del sistema è ad oggi di competenza del Gruppo di coordinamento della supervisione SIS II, di cui fanno parte le autorità di protezione dati dei Paesi membri, – che assicurano la supervisione delle autorità nazionali competenti per il sistema SIS II, e il Gepd, che supervisiona il trattamento dati posto in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (EU-LISA), alla quale è rimessa la gestione del sistema centrale.

Nel corso del 2019 il Gruppo di coordinamento della supervisione SIS II si è riunito due volte, il 19 giugno e il 26 novembre (i documenti sono reperibili presso il sito del Gruppo alla pagina: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en). Nel corso della prima riunione si è riflettuto sugli effetti della Brexit (anche con riferimento alle importanti conseguenze di un eventuale cd. *no deal*) rispetto all'utilizzo del sistema SIS II. A decorrere dal 2021, infatti, il Regno Unito diventerà a tutti gli effetti un Paese terzo e, di conseguenza, a partire da tale data le sue autorità di controllo non potranno più accedere al sistema CSIS. È stato poi affrontato il tema dell'impatto sulla disciplina di protezione dei dati della cd. interoperabilità dei sistemi di informazione di larga scala (l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS e l'ECRIS- TCN) prevista dai due regolamenti, adottati nel maggio 2019, proprio al fine di istituire un quadro per l'interoperabilità tra i sistemi di informazione dell'UE, da un lato, nel settore delle frontiere e dei visti e, dall'altro, nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione (reg. n. 2019/817 e 2019/818). I regolamenti prevedono, tra l'altro, la creazione di un *European Search Portal* (ESP) attraverso cui le autorità competenti degli Stati membri e le agenzie dell'Unione possano ottenere un accesso rapido ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol. L'ESP non fornirà informazioni a cui l'utente non ha accesso ai sensi della normativa nazionale applicabile e dell'Unione.

Nel corso della seconda riunione si è discusso dell'aumento delle richieste di accesso al SIS da parte di Paesi terzi – nonché della proposta di regolamento che

stabilisce le condizioni per l'accesso ad altri sistemi di informazione dell'UE ai fini dell'*European Travel Information and Authorisation System* (ETIAS).

Il Gruppo ha inoltre discusso del futuro della supervisione sul sistema informativo SIS II che, come per gli altri sistemi informativi dell'Unione nei settori delle frontiere, dell'asilo e della migrazione (EES, ETIAS e VIS), della cooperazione di polizia e giudiziaria (SIS, EPPO, Eurojust, ECRIS-TCN) e del mercato interno (IMI), sarà affidato alla Commissione di controllo coordinato sul trattamento dei dati istituita nell'ambito del Cepd (v. *supra*).

Gruppo di supervisione del sistema Eurodac

Il Gruppo di supervisione del sistema Eurodac (i cui documenti sono rinvenibili sul sito internet alla pagina: https://edps.europa.eu/data-protection/european-it-systems/eurodac_en) è competente per assicurare il rispetto della protezione dei dati personali all'interno del sistema istituito per la comparazione delle impronte digitali dei richiedenti asilo. Il Gruppo, riunitosi il 20 giugno e il 27 novembre 2019, ha continuato il lavoro per il perfezionamento del regolamento relativo alle tecniche adottate per la raccolta delle impronte digitali e ha adottato il *report* sui risultati di un questionario sui diritti degli interessati fatto circolare tra gli Stati membri, da cui è emersa una sostanziale uniformità delle procedure adottate per la raccolta delle impronte digitali, per la distribuzione di opuscoli informativi e per assicurare la correzione e cancellazione dei dati.

È stato inoltre concordato il contenuto di un volantino, preparato in collaborazione con la *European Union Agency for Fundamental Rights* (FRA), di ausilio alle autorità che si apprestano a svolgere il processo di raccolta delle impronte sia dei richiedenti asilo che degli altri cittadini extracomunitari a cui possono essere prese (*migrants apprehended at the external border*).

Infine è stato illustrato il programma triennale 2019-2021 ed eletto il nuovo presidente del sottogruppo, la delegata della Grecia Eleni Maragou.

Gruppo di coordinamento della supervisione del Sistema informativo visti (VIS)

Il Gruppo di supervisione VIS è competente per il monitoraggio del sistema d'informazione visti, istituito dalla decisione 2004/512/CE e volto a creare uno spazio di libertà, sicurezza e giustizia senza frontiere interne tramite lo scambio di dati relativi ai visti d'ingresso nello Spazio Schengen tra gli Stati che ne fanno parte. Il funzionamento del VIS è disciplinato dal regolamento (CE) 767/2008 e consiste in una banca dati centrale a livello europeo alla quale sono connesse le interfacce nazionali delle autorità degli Stati Schengen competenti per i visti, tra cui gli uffici consolari e i valichi di frontiera esterni degli Stati.

Il Gruppo di supervisione (i cui documenti sono rinvenibili sul sito internet: https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_en) ha tenuto due riunioni, il 20 giugno ed il 27 novembre, in occasione delle quali è stato discusso il *Work Programme* 2019-2021. Il Gruppo è stato altresì aggiornato dall'Agenzia EU-LISA (*European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*) circa alcuni dati dalla stessa acquisiti monitorando il funzionamento del sistema relativamente al periodo 10 gennaio/30 ottobre 2019 ed è stato aggiornato dalla Commissione sullo stato di avanzamento dei lavori relativi all'entrata in funzione dei sistemi EES *Entry-Exit-System* – sistema che si pone l'obiettivo di registrare in una banca dati unica le informazioni in entrata ed uscita di persone di nazionalità non appartenente all'UE che attraversano i confini esterni dell'Unione – e del sistema ETIAS (*European Travel Information and Authorization System*).

Il Gruppo ha lavorato su un rapporto relativo alla formazione del personale delle autorità nazionali che accedono al VIS sulla base delle risposte pervenute a un precedente questionario fatto circolare in materia e ha adottato un rapporto sull'esercizio dei diritti da parte degli interessati nei diversi Stati membri.

21

SID

Il Sistema informativo doganale è volto a consentire la cooperazione tra le autorità nazionali competenti per la prevenzione, la ricerca e il perseguimento di gravi infrazioni delle leggi nazionali in materia (decisione 2009/917/GAI e della decisione quadro 2008/977/GAI) e quelle competenti a contrastare le violazioni di natura amministrativa (sulla base del regolamento (EC) n. 515/1997, consolidato nel 2008). Per i trattamenti effettuati in ambito di polizia e giustizia, la supervisione è attribuita all'Autorità comune di controllo dogane (ACC Dogane) mentre per la cooperazione di tipo amministrativo la competenza è attribuita al Gruppo di coordinamento della supervisione del Sistema informativo doganale (sito internet alla pagina: https://edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en).

Nel 2019 il Gruppo di coordinamento della supervisione SID si è riunito a Bruxelles il 7 maggio. Il segretariato, in una relazione concernente il piano di lavoro programmato per il biennio 2017-2018, ha rappresentato che quasi tutti gli obiettivi sono stati raggiunti, con particolare riferimento all'adozione di un *format* comune per interrogare il SID, e ha predisposto un questionario relativo alla AFIS *Security Policy*. Sono state inoltre formulate proposte per il nuovo programma di lavoro, che interesserà il biennio 2020-2021, tenendo in considerazione anche eventuali aggiornamenti del quadro legislativo del SID nonché valutando l'opportunità di prevedere sessioni di *training* per coloro che dovranno effettivamente svolgere operazioni di consultazione del Sistema.

21.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa e ad altri gruppi di lavoro internazionali*

T-PD

È proseguita l'intensa attività dell'Autorità nell'ambito del Consiglio d'Europa, in particolare attraverso la partecipazione al Comitato consultivo della Convenzione n. 108/1981, cd. T-PD, presieduto dalla dottoressa Alessandra Pierucci del Garante dal 2016.

Le due riunioni plenarie del Comitato, tenutesi a Strasburgo il 13-14 giugno e il 19-21 novembre – cui si sono come di consueto aggiunte le tre riunioni annuali del *Bureau*, il gruppo ristretto del Comitato –, sono state caratterizzate da un'altissima partecipazione delle Parti, spesso rappresentate da delegazioni nazionali nutrite, composte da rappresentanti provenienti sia dai ministeri sia dalle autorità di protezione dati, segno della crescente attenzione da parte degli Stati nei confronti delle attività del T-PD.

Nel corso dell'anno sono stati adottati importanti documenti e avviata la riflessione su nuove tematiche che saranno oggetto del programma di lavoro del Comitato per il biennio 2020-2021.

Il Protocollo emendativo della Convenzione 108 che ha dato vita alla cd. Convenzione 108+ ha continuato a mantenere un ruolo centrale nelle attività del T-PD e a suscitare largo interesse tra gli Stati come standard globale di protezione dei dati.

Nel corso del 2019, sedici nuovi Stati hanno firmato il Protocollo emendativo, portando a trentotto il numero complessivo di firme. Tra gli Stati firmatari, oltre all'Italia che ha sottoscritto il Protocollo il 5 marzo 2019, si segnalano anche tre Paesi che non fanno parte del Consiglio d'Europa (Argentina, Tunisia e Uruguay), a sottolineare la "vocazione globale" della Convenzione. Nel corso del 2019 si sono anche registrate le due prime ratifiche (Bulgaria e Croazia) del Protocollo. Si tratta di un ottimo risultato, che va tuttavia completato con una tempestiva ratifica del Protocollo emendativo che può entrare in vigore (oltre che nel caso della ratifica di

tutte le attuali Parti della 108), anche ove nei 5 anni successivi all'apertura alla firma si raggiunga la ratifica di almeno 38 Parti.

Sempre con riferimento alla Convenzione 108+, il Comitato ha continuato il lavoro sui meccanismi, la cui competenza sarà attribuita al futuro comitato convenzionale, di valutazione (*evaluation*) dei futuri candidati ad accedere alla 108+ e di periodico riesame (*follow up*) per verificarne la persistente aderenza ai principi della Convenzione stessa. Oltre al documento descrittivo che spiega i meccanismi di *evaluation* e *follow up*, il Comitato ha lavorato su una bozza di questionario che sarà sottoposto a candidati e Parti nell'ambito di tali procedure. Per completare il lavoro sulle procedure è stato deciso di costituire un gruppo di lavoro composto dai componenti del *Bureau* e dalle delegazioni interessate. Tutto ciò tenendo conto del fatto che, se da una parte l'entrata in vigore della Convenzione (tra almeno cinque anni) consentirebbe una riflessione approfondita su tali procedure, dall'altra, la loro finalizzazione appare di fatto più urgente, in base all'art. 36.2 del Protocollo emendativo. Tale disposizione prevede infatti che a partire dall'apertura alla firma del Protocollo (avvenuta il 10 ottobre 2018) qualunque nuova richiesta di accedere alla 108 debba essere accompagnata dalla richiesta di accessione alla 108+ rendendo quindi necessaria una pronta predisposizione dei meccanismi valutativi previsti da quest'ultima.

Il Comitato ha inoltre proseguito le attività previste dal programma di lavoro per l'anno 2019.

All'esito di procedura scritta, il 25 gennaio 2019 sono state adottate le linee guida in materia di intelligenza artificiale e protezione dei dati (*Guidelines on Artificial Intelligence and Data Protection*) che si rivolgono a *policy makers*, sviluppatori e fornitori di servizi fondati sull'intelligenza artificiale (I.A.) e offrono indicazioni affinché l'impiego di tale tecnologia avvenga nel rispetto dei principi della Convenzione 108+. Nonostante quest'ultima non sia ancora entrata in vigore, essa rappresenta ormai il parametro di riferimento delle raccomandazioni e linee guida del T-PD. Tra i punti più significativi delle linee guida in materia di I.A., si segnalano: la necessità di avere un approccio fondato sulla preventiva valutazione dell'impatto che soluzioni I.A. possono avere sui diritti fondamentali, anche in ragione dei possibili effetti discriminatori che possono da essa derivare e l'opportunità di inserire nel processo di valutazione nuove "forme partecipatorie", basate sul coinvolgimento di individui e gruppi potenzialmente interessati dagli effetti dell'I.A. Ciò per evitare che le scelte sull'utilizzo di tali nuove tecnologie, che rischiano di cambiare radicalmente il nostro modo di stare nella società, siano appannaggio esclusivo di chi detiene il sapere tecnologico.

Raccomandazione (2019) 2

Il 27 marzo è stata adottata dal Comitato dei ministri del Consiglio la raccomandazione (2019) 2 sulla protezione dei dati relativi alla salute. L'adozione della Raccomandazione chiude il lungo percorso di revisione della Raccomandazione (97)2 attualizzando i preesistenti principi di tutela dei dati a fronte delle molte sfide determinate dalla diffusione di nuove tecnologie e della digitalizzazione del settore sanitario (T-PD(2018)06rev). Diversamente dall'originaria raccomandazione, che si riferiva ai "dati sanitari", il nuovo documento muove da una più ampia definizione di "dati relativi alla salute" che comprende i dati personali riferibili alla salute mentale o fisica di un individuo, inclusi quelli che riguardano la fornitura di servizi di cura o che rivelano informazioni sulle condizioni di salute pregresse, presenti e future della persona. Specifiche previsioni riguardano le garanzie rafforzate che, in base all'art. 6 della Convenzione 108+, devono assistere i trattamenti di dati sulla salute. Sono previste ulteriori garanzie per il trattamento dei dati genetici (particolarmente sensibili per il loro carattere predittivo), nonché sulla condivisione dei dati di salute

21

del paziente da parte di più professionisti del settore al fine di garantire la migliore assistenza medica nel rispetto dei diritti delle persone. Ulteriori previsioni riguardano l'uso di dati ai fini di ricerca scientifica, in particolare per assicurare il rispetto del principio di trasparenza. Infine, viene affrontata la questione dei sempre più diffusi dispostivi sanitari mobili (impiantati o meno sulla persona) ai quali si applicano tutti i principi della raccomandazione: segnatamente, stringenti misure di sicurezza, obblighi di trasparenza volti ad informare adeguatamente gli interessati, nonché la necessità di adottare strumenti che garantiscano il pieno controllo sui propri dati.

Il tema protezione dei dati e salute è stato al centro anche di un confronto del T-PD – a margine della plenaria di giugno – con lo *Special Rapporteur* delle Nazioni Unite sul diritto alla *privacy* Joe Cannataci, in particolare in merito alla Raccomandazione – predisposta da un'apposita *Task Force* in ambito ONU – sulla protezione e l'uso dei dati relativi alla salute. In tale incontro rappresentanti della *Task Force* e del T-PD si sono confrontati anche al fine di favorire la coerenza delle rispettive raccomandazioni.

Criminalità informatica

Il Comitato ha inoltre proseguito la discussione in merito alle implicazioni sulla protezione dei dati delle revisioni alla Convenzione di Budapest sulla criminalità informatica. A seguito della pubblicazione da parte del Comitato *cybercrime* del Consiglio d'Europa (T-CY) della bozza del secondo protocollo addizionale alla Convezione di Budapest sottoposto a consultazione pubblica, il T-PD ha potuto valutare le disposizioni concernenti l'accesso diretto da parte delle autorità di *law enforcement* di un Paese ai dati personali relativi agli utenti di servizi di telecomunicazione detenuti dai relativi fornitori stabiliti in un altro Paese e all'accesso ai medesimi attraverso altra autorità dello Stato terzo. Nella plenaria di novembre il Comitato ha adottato un parere su tale bozza di protocollo con il quale sono stati messi in evidenza alcuni punti critici del *draft*, e sottolineato che: a) la soluzione ideale nella predisposizione di qualsiasi nuovo quadro di regole per l'accesso ai dati in questione è che le Parti coinvolte siano anche invitate a ratificare la Convenzione 108+ al fine di assicurare adeguate garanzie sul piano della tutela dei diritti; b) ove ciò non fosse possibile, l'auspicio del Comitato è che siano inserite nel protocollo opportune garanzie in linea con la Convenzione 108+. Il parere del Comitato è stato presentato nella sessione dedicata alla protezione dei dati in ambito di giustizia della Conferenza Octopus tenutasi a Strasburgo dal 20 al 22 novembre 2019 che ha riunito ministri, esperti, rappresentanti della società civile, del *business online* e delle autorità di protezione dei dati per discutere del bilanciamento tra le esigenze investigative e la tutela dei diritti fondamentali.

Dopo l'adozione di importanti lavori come quelli citati, il Comitato ha discusso delle tematiche da affrontare nel successivo biennio. La plenaria di giugno ha adottato, su proposta del *Bureau*, il programma di lavoro 2020-2021.

Profilazione

Tra i temi inclusi nel programma e già oggetto di discussione delle successive riunioni del *Bureau* nonché della plenaria di novembre, si segnala la revisione della Raccomandazione (2010)13 in materia di profilazione. Il Comitato ha infatti concordato sull'opportunità di tornare sul tema, anche per tenere conto delle nuove questioni emerse in tema di *Big data* e intelligenza artificiale (entrambi peraltro oggetto di linee guida nel frattempo approvate dal Comitato), delle crescenti forme di profilazione in ambito pubblico, nonché delle più recenti e frequenti tecniche di manipolazione degli utenti della rete fondate sulla raccolta di dati personali (ad es. Cambridge Analytica). Se infatti la raccomandazione del 2010 aveva un ambito di applicazione trasversale, nei fatti ha tenuto in maggiore considerazione la profilazione da parte di soggetti privati in ambito commerciale, trascurando quella effettuata in altri ambiti o da soggetti pubblici.

Il Comitato ha inoltre concordato di includere nel programma di lavoro il tema del riconoscimento facciale, avviando la discussione al riguardo. Con l'ausilio di due esperti, sono state discusse le implicazioni tecniche e giuridiche di tale tecnologia alla luce dei criteri previsti dalla Convenzione modernizzata sui dati biometrici, inclusi nelle categorie particolari di dati che meritano una protezione rafforzata in base all'art. 6 della Convenzione 108+.

Protezione dei dati nei sistemi scolastici

È stata avviata la discussione relativa alle sfide per la protezione dei dati derivanti dall'uso di nuove tecnologie nell'ambito dell'istruzione (dalle piattaforme di *e-learning*, ai registri elettronici, all'impiego di biometria per l'accesso a istituti scolastici) e dalla progressiva tendenza a inserire gli studenti, fin dalla più giovane età, in *cluster* che ne condizionano lo sviluppo. Anche in questo caso il Comitato ha discusso con gli esperti che, oltre a predisporre un *report* sul tema, hanno elaborato una bozza di raccomandazione sulla quale il Comitato continuerà a lavorare in vista dell'adozione di linee guida.

Le due plenarie sono state occasione anche per ulteriori eventi e discussioni. La plenaria di giugno è stata infatti anticipata da una consultazione pubblica sulla raccomandazione in materia di protezione dei dati relativi alla salute lanciata dallo *Special Rapporteur* delle Nazioni Unite sul diritto alla *privacy* Joe Cannataci (11 e 12 giugno), alla quale ha partecipato la presidente del T-PD e alcuni membri del Comitato anche al fine di favorire la coerenza di tale documento con la mensionata raccomandazione CoE (2019)2 e da una conferenza sulla Convenzione 108+, occasione per un interessante confronto sulle implicazioni pratiche e l'importanza della 108+ in un contesto extra-europeo.

Il Comitato ha continuato a cooperare con gli altri comitati del Consiglio d'Europa sugli aspetti di propria competenza, in particolare, come si è detto, con il Comitato *cybercrime*, per ciò che concerne i profili di protezione dati derivanti dall'applicazione della Convenzione di Budapest; con il Comitato della Convenzione Macolin, contro la manipolazione delle gare sportive; con il Comitato sui *Media* e la Società dell'informazione, fornendo un parere sulla bozza di raccomandazione predisposta dallo stesso CD.MSI sull'impatto dei sistemi algoritmici sui diritti umani.

Premio Rodotà

In occasione della Giornata europea della protezione dei dati (28 gennaio 2019) è stato assegnato per la prima volta il Premio Stefano Rodotà istituito dal Comitato per ricordare il grande giurista e primo Presidente del Garante. Il Premio, destinato a ricercatori e studenti allo scopo di valorizzare e dare visibilità a progetti di ricerca innovativi e originali nel campo della protezione dei dati personali sviluppati in ambito universitario, è stato assegnato a Ingrida Milkaite and Eva Lievens per un progetto dedicato ai diritti del minore presentato dalle vincitrici nella plenaria del Comitato; è stata altresì conferita la menzione speciale a Jef Ausloos per il lavoro condotto sul diritto all'oblio.

CAHAI

Con una decisione dell'11 settembre 2019 del Comitato dei ministri è stato costituito l'*Ad Hoc Committee on Artificial Intelligence* (CAHAI). Il Comitato, sulla base di ampie consultazioni con le parti interessate, ha avuto mandato di esaminare la fattibilità e i principali elementi di un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'intelligenza artificiale, basato sulle norme del Consiglio d'Europa in materia di diritti umani, democrazia e stato di diritto. Nell'adempiere a tale compito, il comitato *ad hoc* tiene conto delle norme esistenti in ambito CoE in tale settore, *in primis* le ricordate linee guida in materia di protezione dati e intelligenza artificiale.

Il primo incontro del CAHAI, al quale ha partecipato il Segretario generale del Garante insieme al rappresentante del Mise, si è tenuto a Strasburgo il 18-20

21

novembre. La riunione è stata l'occasione per presentare gli strumenti principali esistenti a livello internazionale e regionale, nonchè per svolgere una prima riflessione sugli elementi e le proposte volte ad indirizzare i lavori del Comitato, in particolare con riferimento alla possibilità che da strumenti di *soft law* si possa passare ad una cornice regolatoria vincolante per le Parti, e sul metodo di lavoro del Comitato.

Il CAHAI, il cui mandato ha una durata di due anni, presenterà un primo rapporto contenente proposte per il Comitato dei ministri entro maggio 2020.

OCSE – WP-DGP

Il Garante ha attivamente partecipato ai lavori dell'OCSE, in seno al WP-DGP, Gruppo di lavoro nato dalla trasformazione del WPSPDE (*Working Party on Security and Privacy in Digital Economy*) in *Working Party on Policies for Digital Data Governance and Privacy* con relativo *spin off* del tema della sicurezza digitale nel neocostituito "*Working Party on Digital Security Policy*" (SDE). Nel corso della prima riunione di novembre 2019 del WP-DGP è stata confermata come vice presidente del *Bureau* per il 2020 la dottoressa Manuela Siano del Garante.

La "ristrutturazione" del WPSPDE si è resa necessaria in quanto, quando il Gruppo WPSPDE è stato creato (nel 1995), la *data governance/privacy* e la *digital security* erano due tematiche emergenti nella maggior parte dei Paesi ed è stato possibile affrontare insieme i due temi e raggiungere una massa critica che ha aumentato la visibilità di ogni area a livello internazionale. Ciò ha permesso all'OCSE di ponderare l'agenda internazionale di entrambe le tematiche per oltre 20 anni e di influenzarle attraverso il lavoro analitico e la produzione di otto raccomandazioni del Consiglio OCSE. Tuttavia negli anni la sicurezza digitale e la *governance* dei dati hanno assunto una tale rilevanza che il doppio mandato del Gruppo di lavoro, che ne era stato un punto di forza, cominciava a limitare la capacità dell'OCSE di fornire sufficiente spazio di discussione a ciascuna area tematica e di elaborare un'agenda strategica altrettanto ambiziosa in entrambi gli ambiti. Pertanto durante la riunione del WPSPDE di maggio 2019 è stata condivisa la necessità di un cambiamento per consentire all'OCSE di mantenere la propria *leadership* in materia di sicurezza digitale e *governance* dei dati/*privacy*. Tale cambiamento si è tradotto nella formazione del citato WP-DGP che raccoglie ora tutte le questioni strettamente dedicate alla sicurezza digitale. Questo Gruppo di lavoro riunisce i responsabili delle politiche di sicurezza digitale dell'OCSE al fine di consentire a questa comunità di: i) fissare l'agenda politica nel settore della sicurezza digitale per la prosperità; ii) sviluppare politiche di sicurezza digitale basate sull'evidenza e una guida pratica per creare fiducia nella trasformazione digitale e sostenere la resilienza, la continuità e la sicurezza delle attività critiche; iii) cooperare, condividere le migliori pratiche e condurre discussioni tra le parti interessate sulla sicurezza digitale.

Revisione delle *Privacy guidelines*

Nel corso delle riunioni del WPSPDE (maggio 2019) e del WP-DGP (novembre 2019) si è dato il via al lavoro di revisione delle linee Guida OCSE sulla *Privacy* (*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*), adottate dal Consiglio OCSE nel 2013. Il neo-costituito gruppo di esperti (PGEG), a cui il Garante partecipa, sta guidando il lavoro di revisione in corso. Si ricorda che le prime *Privacy guidelines* risalgono al 1980 e rappresentano il primo *set* di principi di protezione dati internazionalmente riconosciuti. Contengono le definizioni rilevanti in materia di *data protection* e forniscono otto principi fondamentali per la relativa applicazione nazionale: limitazione della raccolta dati, qualità dei dati, specificazione degli obiettivi, limitazione dell'uso, salvaguardia della sicurezza, apertura, partecipazione individuale e responsabilità (*accountability*). Con la revisione del 2013 è stata riaffermata la validità dei predetti principi che restano la base su cui articolare il nuovo lavoro di aggiornamento. Le *Privacy guidelines* del 2013 sono state adottate in forma di