



OSSERVATORIO SUL CONSIGLIO DEI DIRITTI UMANI N. 2/2019

2. LA DIMENSIONE MULTI-SETTORIALE DEL DIRITTO ALLA RISERVATEZZA E ALLA PROTEZIONE DEL DATO PERSONALE: IL CONTRIBUTO DEL RELATORE SPECIALE SUL DIRITTO ALLA PRIVACY PRESENTATO NEL CORSO DELLA 40 SESSIONE DEL CONSIGLIO DEI DIRITTI UMANI

1. Tentativi definitivi del diritto alla riservatezza e alla protezione del dato personale nel quadro degli apparati e dei sistemi intergovernativi di natura universale e regionale

La definizione della fattispecie giuridica del diritto alla riservatezza e alla protezione del dato personale, nella sua complessità materiale, è stata inclusa in molteplici strumenti convenzionali costitutivi del diritto internazionale dei diritti umani, sulla scorta dell'archetipo rappresentato dalla Dichiarazione Universale dei Diritti dell'Uomo, nella quale, all'art. 12, si statuisce che: «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».

La medesima formulazione è stata riprodotta utilizzando un linguaggio rafforzativo della titolarità soggettiva del diritto in parola nell'art. 17 del Patto Internazionale sui Diritti Civili e Politici, come segue: «1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks».

La necessità di una ulteriore declinazione della fattispecie, tesa a garantire una protezione mirata per alcune categorie di soggetti i quali si trovano in condizioni di peculiare vulnerabilità, ha portato ad esempio ad un'apposita elaborazione dell'art. 16 della Convenzione delle Nazioni Unite sui diritti del fanciullo: «1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks».

La dimensione individuale della titolarità della fattispecie in parola è stata traslata, in tempi più recenti, nel processo negoziale che ha condotto all'adozione ed apertura alla firma della Convenzione internazionale sulla protezione di tutti i lavoratori migranti e dei

membri delle loro famiglie, il cui art. 14 dispone quanto segue: «No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks».

Nella compilazione di numerosi strumenti di portata declaratoria o di carattere multilaterale ad impatto vincolante a carico degli Stati contraenti e membri di apparati e di sistemi intergovernativi a vocazione regionale, la definizione del diritto alla riservatezza e alla protezione del dato personale è stata contraddistinta da soluzioni materiali e formali del tutto simili.

Se si vuol esaminare, a titolo esemplificativo, il solo contesto europeo nella duplice articolazione rappresentata dal Consiglio d'Europa e dall'Unione europea, i tentativi definitivi hanno contribuito ad una formulazione ancor più complessa poiché gli estensori della disposizione hanno inteso operare con la finalità ultima di adattare la definizione stessa e declinarla in una dimensione sia settoriale sia operativa a tutela del titolare, individuale e collettivo.

L'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali prevede che: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». In questa disposizione, dunque, si introduce nel secondo paragrafo la declinazione dell'obbligo statutario di salvaguardia del diritto, il quale è stato letto ed interpretato dalla Corte europea dei diritti dell'uomo e delle libertà fondamentali in una prospettiva sia negativa che positiva. E' importante sottolineare altresì che, nel sistema in oggetto, l'articolazione delle componenti materiali in cui si articola la fattispecie presenta volutamente una portata generica. Ciò ha portato il giudice a preservarne tale connotazione, prevenendo una possibile definizione esaustiva del concetto di vita privata ed, anzi, favorendo l'inclusione e la correlazione tra molteplici aspetti che attengono alla sfera individuale ed all'identità sociale della persona, alle relazioni interpersonali di portata professionale o commerciale, sino ad arrivare nei tempi più recenti ad attribuire una particolare rilevanza al concetto di interesse personale anche nel contesto dello sviluppo delle nuove tecnologie digitali

Nel caso della Convenzione del Consiglio d'Europa per la protezione degli individui in relazione al trattamento automatizzato del dato personale, corredata da un apposito strumento protocollare funzionale per la creazione di autorità di monitoraggio con il mandato precipuo di sorvegliare le modalità del flusso internazionale di dati, l'intervento di 'modernizzazione' attraverso l'adozione di un ulteriore Protocollo di emendamento ha consentito di attualizzarne il dispositivo rispetto al testo originario della Convenzione stessa del 1980 ([STE no. 108](#), oggi la c.d. Convenzione 108+), per tenere in considerazione le sfide derivanti dall'ampio e controverso utilizzo delle nuove tecnologie digitali. In questo recente esercizio, ai sensi dell'Art. 2 del [Protocollo](#), l'Art. 1 della Convenzione è stato revisionato come segue: «The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal

data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy».

In ultimo, il più recente strumento normativo adottato nel quadro del diritto dell'Unione europea, ovvero il [Regolamento](#) (UE) del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), dispone che: «(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (“Carta”) e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (“TFUE”) stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale (“dati personali”) dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche. [...] 4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

Tutti i riferimenti alle formulazioni definitorie del diritto alla tutela della riservatezza e alla protezione del dato personale nei principali strumenti giuridici di portata internazionale e regionale, di natura convenzionale o declaratoria, hanno assunto una specifica rilevanza nell'ambito della *Human Rights Machinery* delle Nazioni Unite a Ginevra ai fini della creazione, da parte del Consiglio dei Diritti Umani, di una procedura speciale con mandato specifico sulla fattispecie in parola con l'intento di consolidare l'apparato normativo sopra richiamato ma anche di approfondire la complessità materiale del diritto e di rafforzarne la salvaguardia a fronte delle presenti e future sfide delle nuove tecnologie digitali.

2. *Aspetti strutturali ed operativi della Procedura Speciale delle Nazioni Unite sul diritto alla privacy*

L'esigenza di declinare il diritto alla *privacy* nel contesto spazio-temporale odierno, caratterizzato da un ampio e pervasivo utilizzo delle tecnologie digitali, è stata fatta propria

dal Consiglio dei Diritti Umani in occasione della compilazione ed adozione della [Risoluzione n. 28/16](#) del 26 marzo 2015.

Invero, in sede di Consiglio l'argomento era stato già affrontato in occasione di un *Panel* convocato appositamente il 12 settembre 2014 a Ginevra con la partecipazione di numerosi attori, istituzionali e non, per discutere sul tema (Doc. [Risoluzione n. 28/39](#) del 19 dicembre 2014) sulla base degli *inputs* ricevuti dall'Assemblea generale delle Nazioni Unite con le Risoluzioni [n. 68/167](#) del 18 dicembre 2013 e [n. 69/166](#) del 18 dicembre 2014, e delineato nella sua articolazione procedurale con Decisione [n. 25/117](#) del 27 marzo 2014 dello stesso Consiglio.

Una prima e più ampia introduzione del tema, declinata nella relazione tra promozione, protezione e godimento dei diritti umani e l'utilizzo della rete Internet, ben esplicitata in un Rapporto prodotto dall'Ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani (Doc. [A/HRC/27/37](#)), ne ha facilitato la migliore trattazione anche in una prospettiva tecnico-giuridica.

Nella Risoluzione n. 28/16, infatti, il Consiglio menziona espressamente il Commento Generale n. 16 del Comitato di controllo del Patto Internazionale sui Diritti Civili e Politici (*Official Records of the General Assembly, Forty-third Session, Supplement No. 40*, Doc. [A/43/40](#), annex VI), a fondamento di un processo mirato ad «identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy [...]» come anche a «discuss and analyse, on the basis of international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices [...]».

In linea con i principali riferimenti giuridici sopra richiamati, il Consiglio muove da una definizione della fattispecie quale diritto umano «according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference», riconoscendo che «[...] the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society». Il Consiglio riflette altresì sulle attuali condizioni in cui la fattispecie possa subire limitazioni («*Deeply concerned* at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights [...]»), ciò nonostante gli Stati, nel poter autorizzare una eventuale compressione del diritto rappresentata dalla raccolta ed utilizzo di dati personali ed informazioni sensibili, devono sempre assicurare il pieno rispetto del diritto internazionale dei diritti umani nel suo complesso.

Il contributo strutturale, funzionale ed operativo del Consiglio dei Diritti Umani in questo contesto è costituito, come si evince dal dispositivo della Risoluzione n. 28/16, dalla creazione di una procedura speciale con mandato specifico, di durata triennale e recentemente rinnovato, sul diritto alla *privacy*.

In particolare, il mandato del Relatore Speciale sul diritto alla *privacy* ricomprende i seguenti aspetti:

- «(a) To gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies;
- (b) To seek, receive and respond to information, while avoiding duplication, from States, the United Nations and its agencies, programmes and funds, regional human rights mechanisms, national human rights institutions, civil society organizations, the private sector, including business enterprises, and any other relevant stakeholders or parties;
- (c) To identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age;
- (d) To participate in and contribute to relevant international conferences and events with the aim of promoting a systematic and coherent approach on issues pertaining to the mandate;
- (e) To raise awareness concerning the importance of promoting and protecting the right to privacy, including with a view to particular challenges arising in the digital age, as well as concerning the importance of providing individuals whose right to privacy has been violated with access to effective remedy, consistent with international human rights obligations;
- (f) To integrate a gender perspective throughout the work of the mandate;
- (g) To report on alleged violations, wherever they may occur, of the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including in connection with the challenges arising from new technologies, and to draw the attention of the Council and the United Nations High Commissioner for Human Rights to situations of particularly serious concern;
- (h) To submit an annual report to the Human Rights Council and to the General Assembly, starting at the thirty-first session and the seventy-first session respectively».

Il Consiglio dei Diritti Umani ha invitato gli Stati membri, gli organismi dello stesso sistema onusiano, gli attori non istituzionali a sostenere il Relatore Speciale nell'esercizio del suo mandato.

3. La multi-settorialità quale elemento portante della Procedura Speciale nell'esercizio del suo mandato

Nello svolgimento del suo mandato, il Relatore Speciale ha ritenuto opportuno confrontarsi e collaborare con altre procedure speciali già esistenti ed operative le quali sono competenti per la promozione e la protezione di fattispecie giuridiche, diritti e libertà, il cui bilanciamento in linea generale e in singole situazioni necessita di essere valutato per evitare di comprimere o violare il diritto alla tutela della riservatezza e alla protezione del dato personale.

In questa prospettiva, dunque, la cooperazione con i Relatori Speciali sulla libertà di opinione e di espressione e sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nel contrasto al terrorismo si è rivelata fondamentale, soprattutto per garantire una effettiva salvaguardia del diritto alla *privacy* nel contesto delle nuove tecnologie digitali, in riferimento alla raccolta ed alla gestione di una evidente mole di dati ed

informazioni personali da parte di operatori localizzati sul territorio di nazionalità del titolare del dato o – come accade sempre più spesso – all'estero.

Inoltre, lo stesso Relatore Speciale ha approntato una metodologia operativa del tutto innovativa, in considerazione di due principali variabili: la necessità di condurre il dialogo e di consultare diverse categorie di soggetti, pubblici e privati, istituzionali e non; la multi-settorialità connaturata al tema oggetto del suo mandato, che presenta una prevalente natura giuridica e che, tuttavia, ha un forte impatto in differenti aree della società odierna, quali ad esempio i settori sanitario, assicurativo, commerciale.

Per tali motivi, accanto all'impegno di presentazione e di discussione del proprio rapporto annuale presso il Consiglio dei Diritti Umani, il Relatore Speciale in esame ha istituito diverse *TASK forces* a partire dal 2016, incaricate di operare nell'ambito di appositi *Thematic Action Streams*, di essere consultate e di essere incaricate per la compilazione di rapporti tematici o settoriali atti ad agevolare la procedura speciale nell'approfondire alcuni aspetti mirati della materia. Le consultazioni sono state condotte nel formato di eventi occasionali o periodici di natura pubblica o riservata, organizzati dal Relatore Speciale a Ginevra o in ambito regionale. Si possono citare a titolo esemplificativo: l'International Intelligence Oversight Forum 2016 (IIOF2016), tenutosi a Bucarest l'11-12 ottobre 2016; la Conferenza sul tema 'Privacy, Personality and Flows of Information', tenutasi a New York il 19-20 luglio 2016; l'IIOF2017 ospitato a Bruxelles il 20-21 novembre 2017; l'evento sul tema 'Privacy, Personality and Flows of Information in the MENA region' tenutosi a Tunisi il 22-23 maggio 2017. Come ovvio, il Relatore Speciale ha aperto anche delle consultazioni *online* chiedendo ai soggetti interessati di trasmettere alla sua attenzione un proprio contributo scritto.

Sulla scorta dei risultati conseguiti, il Relatore Speciale ha potuto presentare, discutere e programmare, a partire dal 2017, i seguenti rapporti *ad hoc*:

1. March 2017 – Report to UN Human Rights Council «First approaches to a more privacy-friendly oversight of government surveillance»
2. October 2017 – Report to UN General Assembly «*Big Data & Open Data*»
3. March 2018 - Report to UN Human Rights Council «Some preliminary options within Internet Governance for an international legal instrument on government surveillance»
4. October 2018 – Report to UN General Assembly «Improving safeguards and remedies for privacy and health data»
5. March 2019 - Report to UN Human Rights Council «Lessons learned for improved safeguards and remedies in effective oversight of government surveillance»
6. October 2019 – Report to UN General Assembly «Profits and Privacy: the monetisation of personal data as a business model and the responsibilities of corporations»
7. March 2020 - Report to UN Human Rights Council «Proportionality, necessity and law in government surveillance, law enforcement and transborder flows of personal data: the effectiveness and improvement of existing legal safeguards and remedies»
8. October 2020 - Report to UN General Assembly «Privacy, Personality and flows of information: a first global overview of the universal right to privacy from the perspectives of time, place and space»
9. March 2021 - Report to UN Human Rights Council «Progress, regress and other dimensions of the effective oversight of government surveillance»
10. October 2021 – Report to the UN General Assembly «The transborder flow of personal data between corporations, law enforcement and surveillance».

4. I principali contenuti dell'ultimo rapporto presentato dalla Procedura Speciale

In occasione della presentazione dei contenuti del suo ultimo rapporto annuale (Doc. [A/HRC/40/63](#) del 27 febbraio 2019) durante i lavori della 40 sessione del Consiglio dei Diritti Umani, il Relatore Speciale ha approfondito un interessante ed assai attuale aspetto della materia, ovvero la correlazione tra diritto alla riservatezza e nuove sfide poste dalla tecnologia nell'assicurare piena difesa e sicurezza a livello nazionale; sono stati illustrati in particolare i risultati delle *TASK forces* tematiche aventi ad oggetto la dimensione della *privacy* in un'ottica di genere, il rapporto tra *privacy* e personalità, la raccolta dei dati personali a fini sanitari.

La considerazione preliminare formulata dal Relatore Speciale poggia su una contraddizione in termini propria delle autorità statuali nella costruzione del rispettivo assetto legislativo, a fronte di una completa e (presunta) effettiva attuazione degli impegni convenzionali assunti rispetto al recepimento del diritto internazionale dei diritti umani. In altre parole, ogni fattispecie giuridica enunciata ad esempio nel Patto Internazionale sui Diritti Civili e Politici non è comprensivamente protetta e promossa se ulteriori misure legislative dispongono in favore di apparati e di strumenti tecnologici invasivi e lesivi della dignità e della sfera riservata della persona, privando quest'ultima di ogni forma di auto-determinazione e di controllo sull'accessibilità e sull'utilizzo dei dati che la riguardano in via diretta. Il Relatore Speciale richiama a tale proposito un pensiero di PAUL SIEGHART (*Privacy and Computers*, Latimer, London, 1976 p. 24): «in a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do». Eppure lo Stato deve essere in grado di misurare preventivamente l'impatto di dette misure legislative, che consentono all'attore sia pubblico sia privato di procedere nella raccolta, gestione e condivisione del dato personale, provvedendo a disciplinare in modo specifico le limitazioni del diritto alla *privacy* sulla scorta del parametro della necessità in una società democratica – ai sensi degli Artt. 14, 21 e 22 del Patto Internazionale sui Diritti Civili e Politici o anche dell'Art. 8 della Convenzione europea dei diritti dell'uomo – ed ancora, come proposto dal Relatore Speciale, in linea con il doppio parametro della necessità e della necessità in una società democratica, richiamando in questa prospettiva i paragrafi operativi della [Risoluzione n. 34/7](#) del Consiglio dei Diritti Umani del 23 marzo 2017 nei quali si dispone che gli «States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality», dunque utilizzando il “essential, four-fold test [che] is then that any legitimate infringement of privacy cannot be: a) arbitrary and must be provided for by law; b) for any purpose but for one which is necessary in a democratic society; c) for any purpose except for those of “national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others”; and, d) the measure must be proportionate to the threat or risk being managed».

In riferimento al tema della protezione della *privacy* declinato alla luce della garanzia di condizioni sicure diffuse e garantite attraverso il funzionamento di apparati e di sistemi di monitoraggio e di sorveglianza, il Relatore Speciale cita il caso Snowden e la conduzione

di attività potenzialmente dannose per la tutela della riservatezza e del dato personale da parte di agenzie nazionali ed internazionali competenti per il mantenimento della sicurezza e dell'ordine pubblico.

E' evidente come numerose iniziative di dibattito e di consolidamento degli strumenti internazionali convenzionali prevenienti e delle misure di regolamentazione regionale ad impatto diretto sugli Stati membri abbiano rappresentato un importante passaggio per una rinnovata riflessione sul tema, recepita in particolare dal sistema giurisdizionale europeo e fatta propria dalla Corte europea dei diritti dell'uomo nei casi [Centrum for Rattvisa vs. Sweden](#) (19 giugno 2018) e [Big Brother Watch and others vs. UK](#) (13 settembre 2018). Tutte le modalità di raccolta e di scambio di dati ed informazioni attraverso le nuove tecnologie digitali – «especially the Internet, smartphones, Big Data analytics, wearables, smart energy, smart cities, etc.» – rendono il titolare vulnerabile di fronte agli attori nazionali ed internazionali, pubblici e privati giacché tali strumenti sono in grado di profilare e di osservare il comportamento individuale in ogni circostanza.

Il Relatore Speciale pone in evidenza due importanti iniziative avviate nel 2018: l'adozione, il 14 novembre 2018, di una [dichiarazione congiunta](#) firmata dai competenti organismi nazionali di controllo del Belgio, della Danimarca, dei Paesi Bassi, della Norvegia e della Svizzera - Parti contraenti della Convenzione del Consiglio d'Europa 'modernizzata' per la protezione degli individui in relazione al trattamento automatizzato del dato personale, relativa al rischio di compressione del diritto nella condivisione del dato tra agenzie di *intelligence* e di sicurezza nazionale; la creazione di un apposito organismo, il Five Eyes Intelligence Oversight and Review Council (FIORC), da parte di cinque Stati partecipanti all'IIOF2018 – Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti – i quali hanno progressivamente introdotto nei rispetti ordinamenti legislativi domestici misure preventive del rischio sopra menzionato.

In relazione al *focus* tematico sulla relazione tra diritto alla *privacy* e dimensione di genere, il Relatore Speciale ha avviato una consultazione che fa seguito alle raccomandazioni formulate dal Consiglio dei Diritti Umani e dall'Assemblea generale – nelle rispettive Risoluzioni n. 34/7 e [A/RES/71/199](#), per «further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups». La consultazione, ora in corso, ha ad oggetto i 'Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics', in linea peraltro con i contenuti del rapporto prodotto dal Relatore Speciale sulla violenza nei confronti delle donne (Doc. [A/HRC/38/47](#) del 18 giugno 2018).

Il nesso logico tra diritto alla *privacy* e personalità individuale è un altro importante sub-tema affrontato dal Relatore Speciale nel suo rapporto annuale, richiamando la dimensione trasversale della titolarità della fattispecie e l'impatto negativo prodotto dalle nuove tecnologie digitali in termini di «inequality, discrimination or marginalisation based on [...] gender, sexual orientation, gender identity, sex characteristics or expression». La procedura speciale si riferisce al c.d. fenomeno della 'cybermisoginy' e, più in generale, del cyber-abuse di cui sono vittime «women, girls, children, LGBTQI individuals and communities especially transgender individuals, activists, gay teachers, human rights defenders, sex workers, and women journalists». Ciò può aver luogo non soltanto nella vita reale, in situazioni nelle quali si assiste con facilità alla violazione della sfera della

riservatezza personale nell'accesso ed utilizzo ai documenti d'identità per il rilascio di servizi pubblici di natura medica, assicurativa, commerciale, ma anche e soprattutto nel mondo virtuale.

La condivisione, consapevole e dunque consensuale, del dato personale non esclude che la persona possa essere destinataria di attacchi diretti da parte di altri utenti che utilizzano i *social media* per comunicare in modo veritiero o che creano profili falsi per sfuggire dall'identificazione ed ampliare l'intensità dell'attacco nei riguardi del soggetto 'categorizzato' e discriminato. D'altra parte lo stesso strumento tecnologico offre oggi numerose possibilità di accesso ed uso dei dati personali in forma mediata, ovvero senza che il titolare ne sia informato ed abbia espresso il proprio consenso a tal fine, ivi inclusa la condivisione di immagini di natura sessuale, il c.d. 'revenge porn', incentivando sentimenti aggressivi ed il ricorso alla violenza nei confronti delle persone in condizioni vulnerabili, tra le quali il Relatore Speciale riserva una speciale attenzione ai gruppi LGBTQI evidenziando che in alcuni Stati membri sono state introdotte importanti misure legislative per incrementare le attività di monitoraggio e di sorveglianza a fini preventivi.

La raccolta e l'analisi del dato personale nell'ambito del sistema sanitario è l'ultimo sub-tema affrontato dal Relatore Speciale in termini di necessità e di proporzionalità rispetto alla garanzia effettiva del diritto alla riservatezza del titolare, in particolare in riferimento alle predette categorie di soggetti vulnerabili in quanto utenti e pazienti: «We all have therefore, very legitimate interests in our dignity and autonomy being protected by the highest available standards in health-data related scenarios».

La tutela del diritto alla riservatezza e la protezione del dato personale sono esaminati, in questo ambito, in diretta correlazione con i principi etici e le regole procedurali che afferiscono all'esercizio della professione medica – quali, ad esempio, la confidenzialità, il pieno consenso informato, la produzione ed adozione di una documentazione chiara ed intellegibile da parte del paziente, la libera scelta del medico. Al contempo l'operatore medico non può non trattare il dato personale e, talora, come si vedrà, deve valutarne una opportuna condivisione ai fini dello sviluppo della ricerca e della conoscenza; e, in una ulteriore e più ampia dimensione, anche gli operatori del settore sanitario non possono non visionare il dato personale per consentire al paziente l'accesso e l'utilizzo dei servizi medici essenziali.

Ad avviso del Relatore Speciale sussistono molteplici criticità nella raccolta, utilizzo e condivisione del dato personale a fini sanitari: come già si ricordava sopra, è fondamentale in via di principio il consenso informato del paziente in funzione sia del trattamento sanitario che della ricerca medica, tuttavia gli aspetti della disciplina legislativa e procedurale sovente non sono chiari ed uniformi e, ad esempio, richiedono differenti assensi da parte del titolare e paziente nei passaggi dello stesso trattamento. La promozione della ricerca medica sulla scorta della conoscenza e dell'utilizzo del dato personale deve poggiarsi, nuovamente, su una disciplina legislativa *ad hoc* rispetto alle misure regolamentari inerenti l'acquisizione del dato medesimo per il trattamento sanitario. Ciò si rivela ancor più vero se la finalità di acquisizione del dato è condotta non dal personale medico ma dagli operatori in campo sociale, sanitario, professionale ed imprenditoriale, dunque per il conseguimento di obiettivi altri, talora, da quelli propri della conoscenza e della ricerca medico-scientifica. L'attribuzione di competenze specifiche ad organismi composti da rappresentanti delle categorie medica e sanitaria, per la definizione di regole base e di procedure atte a regolare il bilanciamento tra riservatezza ed utilizzo del dato, spesso non poggia su un'ampia conoscenza della disciplina giuridica inerente il diritto alla *privacy*. Ciò

implica una evidente criticità soprattutto in considerazione della scarsa anonimizzazione del dato personale nel sistema sanitario nel suo complesso e dunque nella concreta possibilità che esso venga acquisito *de facto* da parte dell'operatore medico e potenzialmente condiviso con un ampio numero di interlocutori, ad esempio nelle banche-dati *online*. In simili circostanze, si comprime in via generale il livello di sicurezza e di protezione del titolare e paziente, e si limitano le possibilità di conoscenza della casistica delle violazioni del diritto alla *privacy* e di accesso a meccanismi rimediali di natura giurisdizionale e non.

In allegato al rapporto, il Relatore Speciale ha presentato un documento-guida nel quale sono contenuti i principali risultati della *TASK force* tematica in forma di principi per la migliore gestione del dato personale di carattere sanitario, ed ha aperto una apposita consultazione pubblica *online* per la ricezione di commenti al testo.

Nella parte conclusiva del rapporto, in ultimo, il Relatore Speciale ha formulato le proprie raccomandazioni all'indirizzo degli Stati membri, del sistema onusiano e degli attori non governativi, sottolineando la primaria esigenza di disciplinare in modo completo ed inequivoco nelle legislazioni nazionali tutti gli aspetti inerenti la materia, con particolare riferimento ai diritti di genere, contemperando i principi della necessità e della proporzionalità propri di un assetto democratico, affidando una specifica e mirata competenza operativa ad organismi di monitoraggio e di controllo, ed auspicando il rispetto del principio «If it's exchangeable, then it's *oversightable* in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders».

5. Focus sul caso Assange

Rispetto alle consuete e periodiche attività proprie del mandato del Relatore Speciale sul diritto alla *privacy*, sembra interessante richiamare in questo Osservatorio una recente azione svolta dalla procedura speciale inerente il caso Assange.

Invero il Relatore Speciale, come accade nello svolgimento delle attività degli altri organismi della *Human Rights Machinery* ginevrina, è stato investito di una duplice competenza: con riferimento al fondatore di Wikileaks, la possibilità di incontrarlo presso la sede dell'Ambasciata del Governo dell'Ecuador a Londra con l'obiettivo ultimo di determinare se nel caso in esame possa essere riscontrata una effettiva violazione del diritto alla *privacy* di Julian Assange; in merito ad un ricorso presentato dal Presidente del Governo dell'Ecuador, Lenin Morena, circa la condivisione di informazioni e dati personali da parte di un sito Internet, con il fine di valutare se anche sotto questo profilo il diritto alla *privacy* del Presidente sia stato compreso.

In merito a questo ultimo aspetto, a seguito della ricezione di una Nota Verbale a firma del Ministro degli Affari Esteri e della Mobilità Umana dell'Ecuador, per il tramite dei competenti uffici onusiani a Ginevra, il Relatore Speciale ha avviato la sua indagine il 2 aprile 2019 ed ha predisposto un documento di risposta, richiedendo all'interlocutore maggiori informazioni e dettagli sul punto.

In relazione al primo aspetto, il 29 marzo 2019 il Relatore Speciale aveva ricevuto una segnalazione, sempre per il tramite della Divisione delle Procedure Speciali dell'Ufficio dell'Alto Commissario per i Diritti Umani, nella quale il *team* di assistenza legale di Julian Assange presentava un reclamo, corredato di prove materiali, in ordine alla violazione del diritto alla *privacy*. A seguito di tale ricezione, il Relatore Speciale si rendeva disponibile per un incontro, anche estemporaneo giacché quel giorno si trovava per altri impegni proprio

nella città di Londra. Per problemi tempistici e senza alcun passaggio formale di carattere amministrativo, questo incontro non ha potuto avere luogo. Il riscontro tardivo da parte di Julian Assange, il 31 marzo 2019, ha permesso di programmare nuovamente l'incontro: tuttavia è stato indispensabile superare alcuni ostacoli di natura burocratica – ed una ulteriore opportunità d'incontro fallita il 2 aprile scorso, ovvero le note ufficiali dell'Ambasciatore del Governo dell'Ecuador presso il Regno Unito prima, del Ministero degli Affari Esteri ecuadoriano poi, ed infine della Rappresentanza Permanente dell'Ecuador presso le Nazioni Unite a Ginevra, per consentire al Relatore Speciale di fissare quale data opzionabile per l'incontro con Julian Assange il 25 aprile 2019.

È chiaro che l'arresto di Assange, l'11 aprile scorso, su richiesta degli Stati Uniti ai fini dell'estradizione per la presunta collaborazione con l'allora soldato Bradley Manning (oggi l'attivista Chelsea Manning) nell'*hackerare* una password per introdursi nei sistemi informatici governativi e sottrarre i documenti, unitamente alla sospensione dello *status* di rifugiato da parte del Governo dell'Ecuador, condizione a cui si aggiunge la reiterata violazione di Assange stesso circa i termini e le condizioni di libertà vigilata, sono tutti elementi che hanno influito sull'incontro del Relatore Speciale con il fondatore di Wikileaks.

Esso si è tenuto il 25 aprile nell'istituto di detenzione di Belmarsh, nel rispetto delle regole di procedura tipiche dei colloqui con i legali del detenuto, dunque nel rispetto del principio di confidenzialità; esso è stato seguito da uno scambio di riflessioni tra il Relatore Speciale ed il *team* di assistenza legale di Assange che prelude a prossime ed ulteriori indagini ed analisi dei materiali raccolti da parte del Relatore stesso.

CRISTIANA CARLETTI