Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

CLAUDIA CINELLI*

SORVEGLIANZA DIGITALE, SICUREZZA NAZIONALE E TUTELA DEI DIRITTI UMANI

SOMMARIO: 1. Introduzione. – 2. L'esercizio della sovranità statale nel ciberspazio. – 3. La sorveglianza digitale e la responsabilità internazionale dello Stato nel contesto della tutela dei diritti umani. – 3.1 Le legislazioni nazionali in materia di sorveglianza digitale. – 3.2. I diritti umani che rischiano di essere lesi. – 3.3. L'obiettivo legittimo della sicurezza nazionale. – 4. Recenti sviluppi volti ad incentivare comportamenti responsabili da parte degli Stati. – 5. Considerazioni conclusive.

1. *Introduzione*

Le operazioni di sorveglianza digitale sono spesso condotte dagli Stati per acquisire dati sensibili e/o informazioni classificate. Con il fine di migliorare la sicurezza nazionale, le tipologie di sorveglianza alle quali gli Stati stanno facendo maggiormente ricorso sono principalmente due: la sorveglianza di tipo mirato e quella di massa. La sorveglianza di tipo mirato è realizzata come conseguenza ad una minaccia imminente che deriva da un individuo o da un gruppo di individui. Quella di massa, invece, è attuata principalmente nell'ambito di strategie ad ampio raggio di difesa dello Stato[1].

* Ricercatore di Diritto internazionale, Università di Pisa.

[1] Si veda, tra i contributi più recenti e specifici, D. GRAY, S. E. HENDERSON (eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge, 2017; T. WETZLING, K. VIETH, *Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations*, Berlin, 2018, reperibile *online* al sito https://www.ohchr.org. Si veda, inoltre, Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2019 sulla Sicurezza ICT in Italia* del 3 ottobre 2019, p. 14 ss., reperibile *online* al sito https://clusit.it/; Forum economico mondale: *The Cybersecurity Guide for Leaders in Today's Digital World*, 25 ottobre 2019, p. 7 ss.; *Global Risk Report 2019*, 15 gennaio 2019, p. 16 ss., entrambi reperibili *online* al sito https://www.weforum.org/. Nonostante l'indubbio interesse suscitato in dottrina e nel pubblico dibattito, in questa sede non ci occuperemo delle questioni sollevate dal lancio di applicazioni telefoniche per monitorare la diffusione della pandemia nota come Covid-19 o SARS-CoV-2. Almeno per quanto riguarda l'Italia, tale applicazione (denominata "Immuni") viene installata solo dietro scelta dei singoli individui: per un primo inquadramento, v. G. DELLA MORTE, *La tempesta perfetta COVID-19. Deroghe alla protezione dei dati personali ed esigenza di sorveglianza massiva*, 30 marzo 2020, reperibile *online* al sito http://www.sidiblog.org/; M. PLUTINO, *Immuni. Un'app rassicurante in punto di tutela di*

Entrambe sono state talvolta considerate come una "abitudine pericolosa"[2], altre volte, invece, come "strumenti preziosi"[3] nella lotta al terrorismo ed altri gravi crimini contro lo Stato. Ad ogni modo, sono generalmente percepite come "atti altamente invasivi"[4] nella sfera degli interessi particolari degli individui[5].

Con la presente indagine ci si propone di analizzare quando la conduzione di tali operazioni sia suscettibile di qualificare la condotta dello Stato come internazionalmente illecita e far sorgere, quindi, la sua responsabilità. A tal fine, occorre studiare la peculiare modalità di esercizio della sovranità statale nello spazio a-territoriale in cui tali misure digitali si realizzano, ossia il ciberspazio[6]. Successivamente, analizzeremo gli obblighi a carico degli

---

diritti ma a forte rischio di esternalità negative, in *Symposium: Privacy and contact tracing*, 28 maggio 2020, reperibile *online* al sito www.medialaws.eu. Altri Stati, come la Cina, hanno recentemente adottato misure di sorveglianza di massa sempre più invasive, come risulta dalla denuncia di Human Rights Watch, *China: Fighting COVID-19 With Automated Tyranny. Government Response Hinged on Invasive New Surveillance Methods*, 1° aprile 2020, reperibile *online* al sito https://www.hrw.org/news. Infine, più in generale, nel contesto dell'uso di nuove tecnologie digitali durante il suddetto stato di emergenza del COVID-19, si rinvia a M. D'AGOSTINO PANEBIANCO, *Covid-19: AI supports the fight, but reduces rights and freedoms*, in *OIDU*, 2020, p. 247 ss.

[2] Alto commissario delle Nazioni Unite per i diritti umani, *The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights,* UN Doc. A/HRC/27/37 del 30 giugno 2014, par. 3. Per successivi rapporti si veda, tra i più recenti, ID., UN Doc. A/HRC/39/29 del 3 agosto 2018.

[3] Sentenza della Corte europea dei diritti umani del 13 settembre 2018, ricorsi nn. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e al.* c. *Regno Unito*; rinvio dinnanzi alla Grande Camera del 4 febbraio 2019.

[4] Sul punto, v. Assemblea generale, UN. Doc. A/RES/68/167 del 21 gennaio 2014, e successive risoluzioni. Tra le altre, con particolare riferimento alla protezione dei diritti umani nell'ambito della lotta antiterrorista, v. ID: UN Doc. A/RES/69/397 del 23 settembre 2014; UN Doc. A/RES/72/180 del 30 gennaio 2018. A tal proposito, occorre richiamare, seppur brevemente, uno tra i più noti eventi che hanno iniziato a sollevare l'attenzione della comunità internazionale (anche) nella materia oggetto del presente studio. Si tratta delle diverse implicazioni conseguenti alle note rivelazioni di Edward Snowden sulla creazione ed uso di un nuovo programma di sorveglianza digitale di massa da parte principalmente dell'Agenzia per la sicurezza nazionale degli Stati Uniti. Tale programma rese possibile l'acquisizione di rilevanti informazioni concernenti gli affari interni di molti Stati (tra cui potenze alleate – come l'Australia, il Brasile, il Canada, oppure alcuni Stati membri dell'Unione europea – nonché la stessa Unione europea) e dei dati personali dei loro cittadini. In particolare, il presidente brasiliano, Dilma Rousseff, affermò davanti all'Assemblea generale delle Nazioni Unite che le misure di sorveglianza statunitensi erano da considerarsi una violazione del diritto internazionale e dei diritti umani. Nello specifico, richiamò la violazione del diritto alla riservatezza e della libertà di opinione e di espressione dei propri cittadini; sul punto v. discorso del presidente, Dilma Rousseff, 68ª sessione dell'Assemblea generale del 24 settembre 2013 disponibile *online* al sito https://gadebate.un.org. Per un primo commento, v. M. MILANOVIC, *Foreign Surveillance and Human Rights: Introduction*, 25 novembre 2013, reperibile *online* al blog *EJIL Talk*, https://www.ejiltalk.org.

[5] Sotto vari profili, come già anticipato, *supra*, nella precedente nota n. 4 in relazione alle rilevazioni di Snowden, le misure di sorveglianza possono essere percepite come "atti altamente invasivi" anche quando realizzate per ottenere informazioni classificate di uno Stato: in altre parole, una forma di spionaggio in tempo di pace. Tale questione già sorgeva a fine anni Novanta come ci ricorda il caso della rete informatica "Echelon" capace di intercettare ogni forma di comunicazione elettronica, ad esempio, comunicazioni diplomatiche, commerciali e private. Sul punto, v. il rapporto del servizio di ricerca del Parlamento europeo, *Echelon Affair. The EP and the global interception system 1998-2002*, novembre 2014, reperibile *online* al sito https://www.europarl.europa.eu. In questa sede non ci occuperemo dei rapporti tra Stati e della possibile qualificazione di un'attività di sorveglianza digitale come un atto illecito di uno Stato a danno di un altro Stato. In argomento, sia consentito rinviare a C. CINELLI, *La disciplina degli spazi internazionali e le sfide poste dal progresso tecnico-scientifico*, Torino, 2020, cap. 4, spec. par. 2.2.

[6] Sebbene la diffusione del prefisso inglese *cyber* sembri ormai consolidata nella nostra lingua, nel presente studio abbiamo optato per l'uso del prefisso italiano "ciber". I termini ciberspazio e spazio cibernetico saranno usati indistintamente. Lo stesso vale per terminologie ad esso connesse, come le operazioni cibernetiche o ciberoperazioni.

Stati in materia di sorveglianza digitale. Sarà approfondito, in particolare, il regime di responsabilità internazionale dello Stato con riferimento agli obblighi esistenti nel contesto della tutela dei diritti umani e delle libertà fondamentali.

Tale approfondimento sarà suddiviso in tre sottoparagrafi. Nel primo sottoparagrafo, studieremo alcuni esempi di legislazioni statali che regolano le operazioni di sorveglianza digitale.

Nel secondo sottoparagrafo, cercheremo di capire quando i possibili effetti prodotti dall'applicazione delle predette legislazioni sulla sfera individuale siano suscettibili di integrare un illecito internazionale. A tal proposito, concentreremo l'attenzione sui diritti e sulle libertà fondamentali che maggiormente rischiano di essere lesi, ossia il rispetto della vita privata, inteso essenzialmente come diritto alla riservatezza, e la tutela della libertà di opinione e di espressione[7].

Nel terzo sottoparagrafo, esamineremo le clausole di limitazione e di restrizione dei menzionati diritti per valutare quando l'interferenza statale persegue l'obiettivo legittimo della sicurezza statale. Nello specifico, ci soffermeremo sull'interpretazione che a tali clausole è stata data nell'ambito dei meccanismi di tutela a livello universale e a livello regionale.

Sulla base dell'analisi compiuta potranno così essere valutati alcuni recenti sviluppi in materia di sorveglianza digitale nell'ordinamento internazionale al fine di verificare le loro implicazioni sotto il profilo della responsabilità dello Stato.

2. *L'esercizio della sovranità statale nel ciberspazio*

Così come definito nello storico lodo relativo all'isola di *Palmas*, il classico concetto di sovranità si sostanzia nel diritto esclusivo di uno Stato di esercitare le sue funzioni di governo effettivo all'interno dei propri confini territoriali[8]. È innegabile che, oggi come allora, l'ordine giuridico internazionale sia "il guardiano" della coesistenza tra Stati; e, che tale coesistenza ruoti intorno al concetto di sovranità territoriale[9]. Oggi più di allora, però, il diritto internazionale si trova ad affrontare problematiche relative all'esercizio della sovranità in ambiti che non rispondono alla logica dei confini territoriali come, ad esempio, il ciberspazio[10].

La prassi internazionale mostra chiaramente che gli Stati affermano la propria sovranità nel ciberspazio senza incontrare obiezioni di principio da parte degli altri soggetti

[7] Si precisa che in questo studio non analizzeremo la questione dell'applicazione extra-territoriale dei diritti umani nel ciberspazio. Inoltre, i riferimenti all'ingerenza sulla sfera individuale da parte dell'industria di sorveglianza saranno contestualizzati nell'analisi dell'obbligo positivo degli Stati di "attivarsi" per evitare abusi perpetrati dal settore privato. Non faremo riferimento, dunque, al tema della "responsabilità sociale dell'impresa" nel contesto della sorveglianza digitale e diritti umani.

[8] Sentenza della Corte permanente di arbitrato del 4 aprile 1928, caso relativo alla *isola di Palmas* (*Olanda* c. *Stati Uniti d'America)*, p. 838.

[9] Ivi, p. 839.

[10] Per una discussione sul tema, *ex plurimis*, si veda D. BETHLEHEM, *The End of Geography: The Changing Nature of the International System and the Challenge to International Law*, in *Eur. Jour. Int. Law*, 2014, p. 9 ss.; D. S. KOLLER, *The End of Geography: The Changing Nature of the International System and the Challenge to International Law: A Reply to Daniel Bethlehem*, ivi, p. 25 ss.; C. LANDAUER, *The Ever-Ending Geography of International Law: The Changing Nature of the International System and the Challenge to International Law: A Reply to Daniel Bethlehem*, ivi, p. 31 ss.

internazionali[11]. Già agli inizi degli anni Novanta, il rapido sviluppo delle tecnologie dell'informazione e della comunicazione rese necessaria la regolamentazione di Internet come mezzo di diffusione di massa diverso dalla stampa, radio e televisione. La riforma delle telecomunicazioni del 1991 degli Stati Uniti è stata uno dei primi esempi in tal senso[12].

Circa un anno dopo dalla sua entrata in vigore, alcune norme della suddetta riforma furono dichiarate incostituzionali dalla Corte suprema per violazione della libertà di parola garantita dal primo emendamento della Costituzione[13]. Ai fini della nostra indagine, la pronuncia in questione risulta interessante per due principali motivi. In primo luogo, in tale occasione la Corte fornì una delle prime descrizioni del fenomeno di Internet, quale rete internazionale di computer tra loro connessi che consente a milioni di persone di comunicare nel ciberspazio e di accedere a vaste quantità di informazioni provenienti da tutto il mondo[14]. In secondo luogo, la Corte mise in luce le principali implicazioni giuridiche di tale fenomeno. A tal proposito, sottolineò che il carattere transfrontaliero di Internet ha come conseguenza la scarsa effettività di strumenti di regolamentazione nazionali a carattere unilaterale[15].

Oggi, dopo quasi trent'anni dalla menzionata sentenza, le politiche e le azioni degli Stati volte a regolamentare i sistemi informatici di informazione e comunicazione continuano ad essere a carattere prevalentemente nazionale e unilaterale. A livello internazionale, infatti, il concetto giuridico di ciberspazio non è ancora stato definito[16]. Per alcuni, una definizione di tale concetto non sembra rilevante ai fini dell'esercizio della sovranità statale. Tale irrilevanza sembra giustificata dal mero fatto che la creazione dello spazio virtuale dipende da strutture localizzate nello spazio fisico dello Stato territoriale[17].

In altre parole, l'esercizio della sovranità nel ciberspazio trova il suo fondamento nel processo di "territorializzazione" della dimensione virtuale[18]. La dottrina maggioritaria spiega

---

[11] Si veda, per tutti, M. N. SCHMITT (ed.), *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*[2], Cambridge, 2017. D'ora in avanti ci riferiremo a tale opera come il "Manuale di Tallin 2.0". Si precisa che quest'ultimo aggiorna ed integra una precedente versione del 2013 su diritto internazionale e guerra cibernetica.

[12] *Telecommunications Act* del 3 gennaio 1996, entrato in vigore il 7 febbraio 1996. Tale riforma fu soggetta a molte critiche da parte di attivisti che consideravano lo spazio cibernetico come spazio indipendente e libero da qualsiasi tipo di ingerenza statale. In particolare, come forma di protesta, il giorno dopo dell'entrata in vigore della menzionata riforma, la Dichiarazione di indipendenza dello spazio cibernetico fu adottata su iniziativa del ciberattivista statunitense, J. P. Barlow, in occasione del Forum economico mondiale a Davos, reperibile *online* al sito https://www.eff.org.

[13] Sentenza della Corte suprema degli Stati Uniti d'America del 26 giugno 1997, *Reno* c. *American Civil Liberties Union*, 521 U.S. 844 (1997).

[14] Ivi, p. 849 ss.

[15] Ivi, p. 885 ss. Nello specifico, la Corte suprema considerò che proibire la diffusione di materiali considerati "nocivi" (pornografici) per i minori di età attraverso una azione repressiva a carattere nazionale sarebbe risultata di scarsa efficacia vista la provenienza transfrontaliera di tali materiali. Pertanto, propose di rafforzare i sistemi di controllo sull'accesso agli stessi attraverso, ad esempio, l'istallazione di un filtro elettronico in grado di permettere ai genitori di delimitare lo spazio cibernetico in cui i figli possono navigare.

[16] Tra i molti autori che trattano tale questione, si veda, N. TSAGOURIAS, *The Legal Status of Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham-Northampton, 2015, p. 13 ss.; Manuale di Tallin 2.0, p. 11 ss. e p. 564.

[17] A. ZIMMERMANN, *International Law and "Cyber Space"*, in *ESIL Reflections*, 2014, reperibile *online* al sito https://esil-sedi.eu.

[18] La giurisprudenza nazionale ha dato un importante contributo al processo di "territorializzazione" del ciberspazio. Infatti, la competenza degli organi giurisdizionali di accertare la commissione di un illecito virtuale dipende generalmente dalla localizzazione di quest'ultimo negli spazi sotto la giurisdizione dello Stato in cui è avvenuta l'operazione di inserimento in rete; oppure, secondo la teoria degli effetti interni, dove si è perfezionato l'eventuale effetto dannoso. Rimane da chiarire la pluri-localizzazione del fatto virtuale, ovvero

questo processo prendendo come punto di riferimento la rappresentazione del ciberspazio elaborata dal Ministro della difesa statunitense[19]. Quest'ultimo configura il ciberspazio come uno spazio a tre livelli: fisico, logico e sociale[20]. Dal basso verso l'alto, il primo livello rappresenta lo spazio fisico sottoposto alla giurisdizione dello Stato "territoriale" in cui sono situate le infrastrutture che creano la dimensione virtuale[21]. In posizione intermedia, il livello logico consiste nei sistemi e processi operativi per mezzo dei quali si creano connessioni virtuali e interattive tra le infrastrutture ed altri dispositivi informatici dislocate nello spazio fisico di uno o più Stati. Per ultimo, il livello sociale è composto dagli utenti, persone fisiche e giuridiche, di tali infrastrutture e dispostivi.

A nostro avviso, tale rappresentazione sembra aiutare a "confinare" visivamente le connessioni virtuali nella dimensione fisica in corrispondenza, da un lato, della locazione delle infrastrutture e, dall'altro, della posizione degli utenti coinvolti nelle operazioni cibernetiche, sia come attori che come destinatari delle stesse. Ciononostante, il processo di "territorializzazione" incontra il proprio limite davanti alla funzione del livello logico del ciberspazio di creare connessioni a-territoriali di intrinseca rilevanza internazionale.

Tale funzione ha portato alcuni a riflettere sulla possibilità di configurare lo *status* giuridico del ciberspazio come quello di un'area al di là della giurisdizione nazionale, al pari di quanto viene affermato con riferimento al continente Antartico, oppure all'alto mare, o anche allo spazio cosmico[22]. Queste tre aree geografiche (e le risorse ivi locate), però, non sono sottoposte alla sovranità di nessuno Stato conformemente a specifici regimi di natura pattizia e/o consuetudinaria che disciplinano ciascuna area. Al contrario, come già osservato, la prassi mostra che gli Stati esercitano sovranità nel ciberspazio.

Basandoci, dunque, sulla "territorializzazione" del ciberspazio, potrebbe essere ipotizzato un parallelismo con la disciplina di aree sottoposte alla giurisdizione nazionale. Il ciberspazio, infatti, non è l'unico spazio che, sebbene sottoposto alla sovranità statale, ha una intrinseca rilevanza internazionale. Basti pensare, tra gli altri, agli stretti utilizzati per la navigazione internazionale ed allo spazio aereo nazionale. L'elemento che accomuna il ciberspazio con quest'ultimi due casi è essenzialmente rappresentato dalla peculiare modalità di esercizio della sovranità statale (e della giurisdizione) da parte degli Stati. Tale peculiarità si evince dal fatto che gli interessi nazionali e quelli internazionali sono tra loro strettamente

---

come risolvere i casi di concorso di giurisdizioni. La diffusone di materiali in Internet si realizza simultaneamente in qualsiasi altro Stato che, a sua volta, potrebbe vantare un titolo di giurisdizione. Inoltre, può accadere che un fatto virtuale considerato lecito nell'ordinamento giuridico di uno Stato sia invece considerato illecito nell'ordinamento giuridico di un altro Stato. Sul punto v. C. FOCARELLI, *Diritto Internazionale*[5], Padova, 2019, p. 317 ss.

[19] Manuale di Tallin 2.0, p. 11 ss.

[20] Ministero della difesa degli Stati Uniti, *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028*, 22 febbraio 2010, p. 7 ss., reperibile *online* al sito https://fas.org.

[21] Si pensi, ad esempio, alla posa di cavi a fibra ottica, ovvero all'installazione di router e antenne, nonché all'uso di satelliti artificiali. Si precisa che nel caso dell'uso di satelliti artificiali, quest'ultimi sono generalmente soggetti alla giurisdizione dello Stato di immatricolazione e/o di lancio. Sul punto, v. Assemblea generale, UN. Doc 1721 B (XVI) del 20 dicembre 1961.

[22] Generalmente considerati *global commons*, nel diritto internazionale manca una definizione giuridica ed un unico regime specifico per la loro regolamentazione. Talvolta, anche il concetto di "informazione" in senso lato è stato annoverato tra i *global commons*. Sul punto, v. UN System Task Team, *Global Governance and Governance of the Global Commons in the Global Partnership for Development beyond 2015*, gennaio 2013, p. 6, reperibile *online* al sito https://www.un.org.

interdipendenti[23].

Per far fronte a questa peculiarità, gli Stati hanno adottato specifici strumenti di cooperazione internazionale che disciplinano la navigazione negli stretti internazionali e nello spazio aereo[24]. Al contrario, la peculiare modalità di esercizio della sovranità nel ciberspazio non è regolamentata da strumenti specifici di cooperazione per la "navigazione cibernetica"[25]. Ciò può implicare importanti problematiche in relazione all'individuazione degli obblighi internazionali a carico degli Stati, soprattutto nel contesto della tutela internazionale dei diritti umani[26].

3. *La sorveglianza digitale e la responsabilità dello Stato nel contesto della tutela internazionale dei diritti umani e delle libertà fondamentali*

La sempre più frequente adozione, da parte degli Stati, di misure di sorveglianza digitale nei confronti di individui o gruppi di individui, non è passata inosservata agli organismi internazionali istituiti per la protezione dei diritti umani, a livello universale e regionale.

---

[23] Si pensi agli stretti internazionali che includono il mare territoriale di uno o più Stati costieri (come, ad esempio, lo stretto di Messina o lo stretto di Malacca). L'interesse internazionale consiste nella libertà di tutti gli Stati di transitare con le proprie navi attraverso questi bracci di mare strategicamente importanti, anche se, in tutto o in parte, sottoposti alla sovranità nazionale (v., tra gli altri, U. LEANZA, *Il diritto degli spazi internazionali. La tradizione*, vol. 1, Torino, 1999, p. 312 ss. e 343 ss.; Y. TANAKA, *The International Law of the Sea*[3], Cambridge, 2019, p. 116 ss.) Dall'altro lato, la sovranità nello spazio aereo nazionale è esercitata essenzialmente al fine di realizzare gli interessi nazionali ed internazionali nel contesto del funzionamento dei servizi e del traffico aereo (v. T. BUERGENTHAL, *Law-Making in the International Civil Law and ICAO*, Syracuse N.Y., 1969, p. 55 ss.; J. A. CARRILLO-SALCEDO, *Curso de derecho internacional público*, Madrid, 1991, p. 255 ss.).

[24] Il regime degli stretti internazionali è codificato nella parte III della Convenzione delle Nazioni Unite sul diritto del mare, adottata a Montego Bay il 10 dicembre 1982, entrata in vigore il 16 novembre 1994. Attualmente, hanno ratificato o aderito alla Convenzione 167 Stati parti, oltre all'Unione europea. Dall'altro lato, lo spazio aereo è regolamentato da un fitto intreccio di regole pattizie a carattere bilaterale e/o multilaterale, molte delle quali adottate nell'ambito dell'Organizzazione internazionale dell'aviazione civile, istituita il 7 dicembre 1944 mediante l'adozione della Convenzione sull'aviazione civile internazionale. Attualmente, 193 Stati hanno ratificato o aderito alla Convenzione.

[25] Occorre sottolineare che l'agenzia specializzata delle Nazioni Unite, oggi denominata Unione internazionale delle telecomunicazioni, gestisce essenzialmente la ripartizione mondiale delle radiofrequenze e delle orbite dei satelliti di telecomunicazione. Oggi consta di 193 Stati parte e collabora con oltre 900 imprese, università ed altre organizzazioni internazionali, a livello universale e regionale. Il sistema giuridico dell'Unione include strumenti vincolanti per gli Stati parte: la Costituzione e la Convenzione dell'Unione internazionale delle telecomunicazioni e, infine, i Regolamenti amministrativi che integrano la Costituzione e la Convenzione. V., tra gli altri, Manuale di Tallin 2.0, p. 284 ss.; M. SHAW, *International Law*[8], Cambridge, 2018, p. 407 ss.

[26] Occorre ricordare che il settore della criminalità informatica è stato tra i primi che hanno destato l'attenzione internazionale e costituisce oggi l'unico ambito in cui gli Stati hanno adottato specifici obblighi internazionali in relazione ad azioni condotte nel/attraverso il ciberspazio. A tal proposito, la Convenzione sulla criminalità informatica, adottata a Budapest il 23 novembre 2001, entrata in vigore il 1° luglio 2004, è stata ratificata, ad oggi, da 65 Stati, di cui 21 sono Stati non membri del Consiglio d'Europa. Seppur di innegabile valore giuridico, l'ambito di applicazione della menzionata Convenzione è limitato alle sole ciberoperazioni qualificabili come crimine informatico secondo il diritto penale interno di ciascuno Stato parte. A corollario, sono apprezzabili le iniziative dell'Unione europea in materia di criminalità informatica tramite i servizi offerti dall'agenzia Europol, così come nel più ampio contesto della sua strategia digitale. Tra i documenti più recenti, cfr. Commissione Europea, *Shaping Europe's Digital Future*, Luxembourg, 2020.

Tra gli organi sussidiari dell'Assemblea generale delle Nazioni Unite, nel 2015, è stato istituito, per la prima volta, il relatore speciale sul diritto alla riservatezza[27]. Il lavoro svolto da quest'ultimo, parallelamente a quello del relatore speciale sulla libertà di opinione e di espressione[28], è complementare a quello di altri organismi che nelle Nazioni Unite si occupano di diritti umani, come il Comitato dei diritti umani e l'Alto commissario per i diritti umani[29]. Anche i sistemi regionali hanno svolto un ruolo importante grazie soprattutto alla presenza di organi giurisdizionali, come la Corte europea dei diritti umani[30], e di altri meccanismi di monitoraggio, tra cui, il sistema interamericano di promozione e protezione dei diritti umani[31].

3.1. *Le legislazioni nazionali in materia di sorveglianza digitale*

Un'indagine sulle legislazioni nazionali in materia di sorveglianza digitale nei confronti di individui o gruppi di individui consente di individuare tre principali gruppi di Stati.

Il primo gruppo è composto da Stati che, come la Germania, la Svezia e, quanto meno per una prima fase, il Regno Unito[32], si sono dotati di disposizioni interne relative alla sorveglianza digitale che possono essere considerate conformi al diritto internazionale dei diritti umani.

Tra le altre, nella sua recente sentenza del giugno 2020 relativa al caso *P.N.* c. *Germania*, la Corte europea dei diritti dell'uomo ha considerato legittime le misure di sorveglianza di

---

[27] Consiglio dei diritti umani, *Resolution adopted by the Human Rights Council. Right to Privacy in Digital Era*, UN Doc. A/HCR/RES/28/16 del 1° aprile 2015.

[28] Il primo relatore speciale sulla libertà di opinione e di espressione fu istituito nel 2008. V. Consiglio dei diritti umani, *Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HCR/RES/7/36 del 28 marzo 2008.

[29] Alto Commissario per i diritti umani: UN Doc. A/HRC/27/37, cit.; UN Doc. A/HRC/29/39, cit.

[30] V. Divisione ricerca della Corte europea dei diritti umani, *Internet: Case-Law of the European Court of Human Rights*, giugno 2015, p. 5 ss., reperibile *online* al sito https://www.coe.int. Si veda inoltre, tra le più recenti schede informative della Corte europea dei diritti umani, *Factsheet – Access to Internet and Freedom to Receive and Impart Information and Ideas*, giugno 2020, reperibile *online* al sito https://www.echr.coe.int. In dottrina, per uno studio sulla prassi giurisprudenziale in particolare della Corte europea, nonché di altri organi di garanzia, in relazione all'effettiva attuazione del diritto alla libertà d'informazione e di accesso alla rete di Internet, v. M. CASTELLANETA, *La libertà di stampa nel diritto internazionale ed europeo*, Bari, 2012; A. BUSACCA, *Il "diritto di accesso" alla rete di Internet*, in *Rivista OIDU*, 2017, p. 345 ss.

[31] V. Commissione interamericana dei diritti umani, *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*, 21 giugno 2013, adottata congiuntamente dai relatori speciali sulla libertà di opinione e di espressione delle Nazioni Unite e della Commissione interamericana; ID., *Estándares para una Internet libre, abierta e incluyente. Relatoría especial para la libertad de expresión de la Comisión interamericana de derechos humanos*, Doc. CIDH/RELE/INF.17/17 del 15 marzo 2017, p. 83 ss. Più recentemente, si veda anche la dichiarazione congiunta tra i due predetti relatori speciali e l'Organizzazione per la sicurezza e cooperazione in Europa (OSCE), *Declaración conjunta sobre libertad de expresión y elecciones en la era digital*, 30 aprile 2020. I menzionati documenti sono reperibili *online* al sito http://www.oas.org.

[32] Si veda, per il Regno Unito, la sentenza della Corte europea dei diritti dell'uomo del 10 maggio 2010, ricorso n. 26839/2005, *Kennedy* c. *Regno Unito*. La riforma del sistema inglese del *Investigatory Powers Act 2016* ha suscitato aspre critiche, v. Alto Commissario dei diritti umani, *Is International Human Rights Law Under Threat?*, 26 giugno 2017, reperibile *online* al sito https://www.ohchr.org. Si specifica, inoltre, che anche nella sentenza *Big Brother Watch e al.* c. *Regno Unito*, cit., la Corte sottolinea, in termini generali, la presunzione di legittimità delle misure di sorveglianza quale "strumento prezioso" per raggiungere gli obiettivi legittimi della sicurezza nazionale (ivi, par. 386). A differenza del caso *Kennedy,* la Corte europea questa volta accerta l'avvenuta violazione degli artt. 8 e 10 della Convenzione europea da parte del Regno Unito, rispettivamente la tutela della sfera privata e la libertà di espressione (*infra*, par. 3.3).

tipo mirato adottate dallo Stato tedesco nei confronti del ricorrente, il signor P.N.[33]. Nello specifico, si tratta di misure di polizia di natura preventiva adottate nel quadro della lotta alla criminalità, tra cui, la raccolta di dati identificativi (per esempio, fotografie, tatuaggi, impronte digitali, descrizione del profilo personologico) nei confronti di individui che, come il signor P.N., hanno una pregressa condotta criminosa[34].

Parimenti, anche la sentenza *Centrum För Rättvisa* c. *Svezia* della Corte di Strasburgo è emblematica nel contesto, questa volta, delle misure di sorveglianza di massa[35]. Il caso verte sull'accertamento della responsabilità della Svezia con riguardo alla normativa interna sul sistema di intercettazioni e spionaggio elettronico di massa. Anche in questo caso, la Corte ha ritenuto che nel complesso il sistema svedese fornisce garanzie adeguate e sufficienti contro l'arbitrarietà ed il rischio di abusi. Da ciò consegue la constatazione che la mera esistenza di una simile normativa interna non implica, di per sé, un'interferenza illegittima sui diritti tutelati dalla Convenzione europea dei diritti dell'uomo[36].

Il secondo gruppo comprende Stati che – come la Francia[37], l'Italia[38], gli Stati Uniti[39] e molti altri[40] – hanno adottato disposizioni interne non conformi, in tutto o in parte, al diritto internazionale dei diritti umani.

Lo Stato italiano, ad esempio, è stato di recente invitato, in occasione della sesta relazione periodica del Comitato per i diritti umani del 2017, a rivedere la normativa interna nella parte in cui consente alle autorità governative di condurre, senza autorizzazione giudiziaria, le attività di intercettazioni delle comunicazioni personali, nonché di *hacking* e conservazione dei dati personali. Allo stesso tempo, è stato richiesto all'Italia di adottare le misure necessarie per garantire che tutte le imprese nel settore delle tecnologie dell'informazione e della comunicazione sottoposte alla giurisdizione italiana, rispettino le norme sui diritti umani, anche quando si impegnano in operazioni all'estero[41]. Anche al fine di tener conto di tali rilievi, il legislatore italiano è di recente intervenuto sulla normativa in questione prevedendo, tra l'altro, un ruolo maggiore all'autorità giudiziaria per evitare abusi della polizia giudiziaria e ingerenze statali ingiustificate[42].

---

[33] V. sentenza della Corte europea dei diritti dell'uomo del 11 giugno 2020, ricorso n. 74440/17, *P.N.* c. *Germania*.

[34] Nel caso preso in considerazione, il signor P.N., cittadino tedesco, lamentava la violazione dell'art. 8 della Convenzione europea, per aver la polizia disposto la raccolta dei suddetti dati. La Corte considera che non vi sia stata violazione del suddetto articolo (ivi, par. 91). Si veda, *infra*, par. 3.3.

[35] Sentenza della Corte europea dei diritti dell'uomo del 19 giugno 2018, ricorso n. 35252/2008, *Centrum För Rättvisa* c. *Svezia*; rinvio dinnanzi alla Grande Camera del 4 febbraio 2019.

[36] Ivi, par. 90 ss., par. 112.

[37] Comitato dei diritti umani, *Concluding Observations: France*, UN Doc. CCPR/C/FRA/CO/5 del 17 agosto 2015.

[38] Comitato dei diritti umani, *Concluding Observations: Italy*, UN Doc. CCPR/C/ITA/CO/6 del 1° maggio 2017.

[39] Comitato dei diritti umani, *Concluding Observations: United States of America*, UN Doc. CCPR/C/USA/CO/4 del 23 aprile 2014.

[40] Per una rassegna delle osservazioni conclusive del Comitato dei diritti umani sui rapporti periodici presentati dagli Stati, v. Y. SHANY, *On-Line Surveillance in the case-law of the UN Human Rights Committee*, 13 luglio 2017, reperibile *online* al sito https://csrcl.huji.ac.il/blog. Si veda inoltre, *infra*, par. 3.3.

[41] Comitato dei diritti umani, *Concluding Observations: Italy*, cit., parr. 36-37.

[42] Si precisa che nella Gazzetta Ufficiale n. 305 del 31 dicembre 2019 è stato pubblicato il D.L. 30 dicembre 2019, n. 161 (Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni), diventato legge il 20 febbraio 2020, che rivede in parte il sistema delle intercettazioni conformemente alle osservazioni del Comitato. Nello stesso numero della Gazzetta Ufficiale è stato pubblicato anche il D.L. 30 dicembre 2019, n. 162 (Disposizioni urgenti in materia di proroga di termini legislativi, di organizzazione delle pubbliche amministrazioni, nonché di innovazione tecnologica, il c.d. Milleproroghe 2020) che prevede alcune modifiche finalizzate a predisporre il perimetro di sicurezza nazionale cibernetica (ivi, art. 27).

Il terzo gruppo è composto da Stati che – come la Colombia, il Messico, lo Stato degli Emirati Arabi ed altri Stati, soprattutto africani ed asiatici[43] – non si sono dotati di una apposita legislazione nazionale in materia di sorveglianza digitale. Questi Stati sembrano trarre vantaggio da tale vuoto normativo così da utilizzare i sistemi di sorveglianza acquistati dal settore privato per fini diversi da quelli inizialmente predisposti, ovvero per avviare partenariati con l'industria in modo da perpetrare, proprio attraverso quest'ultima, ingerenze arbitrarie sui propri cittadini.

La mancanza di una specifica regolamentazione permette, dunque, di impiegare i sistemi privati di sorveglianza per colpire indirettamente giornalisti, attivisti, figure dell'opposizione e altri individui che svolgono ruoli rilevanti nella società civile, oltre che far fronte (o con la scusa di far fronte), ad esempio, alla lotta al terrorismo ed al narcotraffico[44].

Tra i casi che hanno fatto più scalpore, oltre alle molte denunce contro i diversi sistemi di intercettazione utilizzati dalla Colombia[45], è senza dubbio quello del programma *Pegasus* di una impresa israeliana, il gruppo *NSO*, venduto al Messico e che sembra aver consentito alle autorità messicane la realizzazione di attività di sorveglianza di tipo mirato nei confronti di giornalisti e dissidenti con ingerenze non trascurabili sul godimento dei diritti e delle libertà fondamentali di questi ultimi[46].

In aggiunta, è interessante far riferimento ai partenariati che gli Stati hanno realizzato con l'industria privata (nazionale e non) basati sul sistema della cosiddetta "porta girevole"[47]. Tale sistema permette a funzionari pubblici, esperti dei sistemi di *intelligence* nazionali, di "girare" le proprie competenze al settore privato. Nello specifico, attraverso il denominato Progetto *Raven*, esperti americani del settore delle tecnologie dell'informazione e della comunicazione, già dipendenti della Agenzia di sicurezza degli Stati Uniti, sono stati ingaggiati per prestare servizio presso enti di sorveglianza privata che, a loro volta, fornivano aiuto e supporto al governo dello Stato degli Emirati Arabi Uniti nella conduzione di attività di monitoraggio di attivisti per i diritti umani, giornalisti e rivali politici della monarchia saudita[48].

---

[43] V. *The Million Dollar Dissident; NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender,* 24 agosto 2016; *NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases,* 29 ottobre 2019, entrambi reperibili *online* alla piattaforma della Università di Toronto, https://citizenlab.ca. Occorre richiamare, inoltre, la prassi della Cina nel contesto della sorveglianza massiva già denunciata da organizzazioni non governative, tra cui, Human Rights Watch, *Data Leviathan: China's Burgeoning Surveillance State*, 16 agosto 2019, reperibile *online* al sito https://www.hrw.org/.

[44] Consiglio dei diritti umani, *Report of the Special* Rapporteur *on the Promotion and Protection of the Right to Freedom of Opinion and Expression on His Mission to Mexico*, *David Kaye,* UN Doc. A/HRC/38/35/Add.2 del 12 giugno 2018, parr. 52-55.

[45] Cfr. Commissione interamericana dei diritti umani, *Informe anual de la Comisión Interamericana de derechos humanos 2004*, cap. 4, spec. par. 6 ss.; ID., *Informe anual de la Comisión Interamericana de derechos humanos 2009*, cap. 4, spec. par. 9 ss.; ID., *Informe anual de la Comisión Interamericana de derechos humanos 2014*, cap. 4, spec. par. 1 ss. Più recentemente, si veda il comunicato stampa, *La CIDH y su Relatoría Especial para la Libertad de Expresión exhortan al Estado de Colombia a establecer una investigación diligente, oportuna e independiente respecto a las denuncias sobre espionaje ilegal a periodistas, operadores de justicia, personas defensoras de derechos humanos y líderes políticos*, 21 maggio 2020. I documenti sono reperibili *online* al sito https://www.oas.org.

[46] Consiglio dei diritti umani, UN Doc. A/HRC/38/35/Add.2, cit., par. 55. Le indagini sono attualmente in corso a livello interno anche se sembrano non poter garantire il rispetto dei requisiti di indipendenza e trasparenza.

[47] Consiglio dei diritti umani, *Surveillance and Human Rights. Report of the Special* Rapporteur *on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, UN Doc. A/HRC/41/35 del 28 maggio 2019, par. 20.

[48] *Ibid.*

La panoramica compiuta mostra, dunque, quanto sia evidente, già dall'esame delle varie tipologie di legislazioni nazionali e, comunque, della prassi seguita a livello statale in materia di sorveglianza digitale nei confronti di individui o di gruppi di individui, il rischio che le operazioni in questione provochino effetti negativi sul godimento di alcune garanzie individuali. Sulla base di tale constatazione, è opportuno a questo punto evidenziare quali sono i diritti che con maggiore plausibilità possono essere lesi in conseguenza delle citate misure di sorveglianza digitale.

3.2 *I diritti umani che rischiano di essere lesi*

I diritti umani che risultano maggiormente lesi dalle misure di sorveglianza digitale poste in essere da parte degli Stati sono il diritto alla tutela della sfera privata, nella sua accezione di diritto alla riservatezza, e la libertà di opinione e di espressione. In particolare, il diritto alla riservatezza è stato interpretato come "porta d'accesso" per il godimento di almeno una delle due menzionate libertà[49].

Il diritto alla tutela della sfera privata e la libertà di opinione e di espressione sono riconosciuti nella Dichiarazione Universale dei diritti dell'uomo del 1948[50], agli articoli 12 e 19, rispettivamente; successivamente, sono stati codificati da strumenti pattizi a carattere universale e regionale[51]. I loro contenuti normativi sono stati poi ampliati nel tempo grazie all'interpretazione evolutiva sviluppata nell'ambito dei diversi meccanismi giurisdizionali e quasi-giurisdizionali istituiti a tutela dei diritti umani.

Iniziando dal diritto al rispetto della sfera privata, il contributo degli organismi istituiti a tutela dei diritti umani nell'ambito delle Nazioni Unite[52] e dei sistemi regionali, in particolare

---

[49] Commissione interamericana dei diritti umani, *Libertad de expression e Internet*, Doc. OEA/Ser.L/V/II.CIDH/RELE/INF. 11/ del 31 dicembre 2013; Consiglio dei diritti umani: *Report of the Special* Rapporteur *on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UN Doc. A/HRC/23/40 del 17 aprile 2013, par. 3; *Report of the Special* Rapporteur *on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye,* UN Doc. A/HRC/29/32 del 22 maggio 2015, parr. 16-18. Per un recente commento più generale sulle implicazioni delle ciberoperazioni nel contesto della tutela dei diritti umani, v. F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, spec. p. 260 ss.

[50] Dichiarazione Universale dei diritti dell'uomo adottata dall'Assemblea generale, UN Doc. A/RES/217A(III) del 10 dicembre 1948.

[51] A livello universale, si vedano, rispettivamente, gli artt. 17 e 19 del Patto internazionale sui diritti civili e politici, adottato dall'Assemblea generale, UN Doc. 2200A(XXI) del 16 dicembre 1966, entrato in vigore il 23 marzo 1976. Per alcuni esempi a livello regionale, si vedano, rispettivamente, gli artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, adottata a Roma il 4 novembre 1950, entrata in vigore il 3 settembre 1953; gli artt. 11 e 13 della Convenzione americana dei diritti umani, adottata a San José il 22 novembre 1969, entrata in vigore il 18 luglio 1979; gli artt. 4 e 9 della Carta africana dei diritti umani e dei popoli, adottata a Nairobi il 28 giugno 1981, entrata in vigore il 21 ottobre 1986. Per un recente commento sul sistema africano di protezione dei diritti umani, si rinvia a P. GARGIULO, *La tutela internazionale dei diritti dell'uomo nel continente africano*, Napoli, 2017; E. CASTRO, *Libertà di espressione e censura nell'interpretazione della Commissione africana nel caso Open Society Justice Initiative*, in *OIDU*, 2020, p. 163 ss.

[52] Per citarne alcuni tra i più rilevanti, v. Comitato dei diritti umani, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc. HRI/GEN/1/Rev.9 (vol. I) del 8 aprile 1988; vedi anche, più recentemente, la risoluzione dell'Assemblea generale, *Resolution on the Right to Privacy in the Digital Age*, UN Doc. A/RES/73/179 del 17 dicembre 2018; Consiglio dei diritti umani: UN Doc. A/HCR/RES/28/16, cit.; *Report of the Special* Rapporteur *on the Right to Privacy in Digital Era*, *Joe Cannataci*, UN Doc. A/HCR/RES/40/63 del 27 febbraio 2019; e, Alto commissario delle Nazioni Unite per i diritti umani: UN Doc. A/HRC/27/37, cit.; UN Doc. A/HRC/39/29, cit.

quello europeo e interamericano[53], indica chiaramente che tale diritto include la tutela della riservatezza (e dei dati personali).

La giurisprudenza evolutiva sulla tutela alla riservatezza è stata presa in considerazione nel processo di codificazione di strumenti regionali più recenti, come la Carta dei diritti fondamentali dell'Unione europea del 2001, giuridicamente vincolante dal 2009[54], dove il diritto alla protezione dei dati di carattere personale è riconosciuto esplicitamente dal suo articolo 8, mentre il diritto al rispetto alla vita privata è sancito nell'articolo 7. Inoltre, tra gli sviluppi più recenti in materia di tutela della riservatezza, deve essere ricordato il Regolamento generale dell'Unione europea sulla protezione dei dati personali[55].

Il Regolamento non fa specifico riferimento all'acquisizione dei dati nel contesto della realizzazione di misure di sorveglianza digitale adottate dagli Stati membri dell'Unione per migliorare la loro sicurezza nazionale. In linea più generale, si limita a segnalare che quando le attività di trattamento dei dati personali riguardano il monitoraggio del comportamento di soggetti che si trovano nell'Unione, il Regolamento si applica nella misura in cui tale comportamento ha luogo all'interno dell'Unione[56]. Inoltre, specifica che la sorveglianza sistematica su larga scala di una zona accessibile al pubblico debba essere sottoposta ad una previa valutazione d'impatto sulla protezione dei dati[57].

Proseguendo con l'analisi dei contenuti normativi della libertà di opinione e di espressione, è possibile individuare una distinzione concettuale tra le due libertà, nonostante

---

[53] V. Consiglio d'Europa, *Guide on Article 8 of the Convention –Right to Respect for Private and Family Life*, 31 agosto 2019, reperibile *online* al sito https://www.echr.coe.int. Non va comunque dimenticato che, traendo diretta ispirazione dalla tutela della sfera privata dell'art. 8 della Convenzione europea, la Convezione n. 108 del Consiglio d'Europa del 1981 è stato uno dei primi strumenti normativi in materia di trattamento automatizzato dei dati personali, aperta alla ratifica anche a Stati non membri del Consiglio d'Europa e ad altre organizzazioni regionali come l'Unione europea, che l'ha ratificata nel 1999. Nel maggio 2018 il Consiglio d'Europa ha adottato un protocollo di modifica del testo della menzionata Convenzione n. 108. Tale Protocollo non è ancora entrato in vigore.

Per quanto riguarda il sistema interamericano, la Corte di San José ha interpretato in modo estensivo l'art. 11 della Convenzione americana dei diritti umani, in cui è riconosciuto il divieto di interferenze arbitrarie nella vita privata, incluso nella "corrispondenza". La predetta Corte ha esplicitamente riconosciuto che il termine "corrispondenza" fa riferimento anche a nuove tipologie di comunicazione attraverso le tecnologie dell'informazione e della comunicazione, come Internet. Pertanto, la protezione della vita privata in relazione alle diverse forme di comunicazione implica la protezione dei dati personali. Si veda, ad esempio, già nel 2009 le sentenze della predetta Corte, il caso *Tristán Donoso* c. *Panamá*, sentenza del 27 gennaio 2009, par. 121 e par. 202 ss.; ed il caso *Escher y otros* c. *Brasil*, sentenza del 6 luglio 2009, par. 239 ss. Per un quadro complessivo e più recente, si rinvia al rapporto redatto da alcune associazioni per la difesa dei diritti umani, TEDIC e al., *La adquisición y el abuso de tecnologías de vigilancia en América Latina* del 15 febbraio 2019, reperibile *online* al sito https://www.tedic.org.

[54] La Carta dei diritti fondamentali dell'Unione europea, proclamata solennemente nel 2000 a Nizza dal Parlamento, dal Consiglio e dalla Commissione, ha acquisito carattere giuridicamente vincolante solo il 1° dicembre 2009, con l'entrata in vigore del Trattato di Lisbona, così come oggi previsto dall'art. 6, comma 1, del Trattato sull'Unione europea.

[55] Regolamento (UE) 2016/679 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*, in *GUUE* L 119/1 del 4 maggio 2016. In dottrina, tra gli altri, per una evoluzione dell'ordinamento dell'Unione in materia, v. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in L. PANELLA (a cura di), *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, Napoli, 2018, p. 13 ss.

[56] *Ivi*, art. 3 (b). Per commento più generale, si rinvia a A. BONFANTI, *Intercettazione di comunicazioni telematiche e acquisizione di dati: sullo studio dell'Unione europea su Legal Frameworks for Hacking by Law Enforcement*, in *Dir. um. dir. int.*, 2017, pp. 506 ss.

[57] Art. 35, comma 3 (c) del Regolamento (UE) 2016/679, cit.

la loro stretta correlazione. In particolare, la libertà di opinione, intesa come libertà di avere un'idea e di svilupparla a titolo di ragionamento personale, è assoluta e incondizionata. Di conseguenza, qualsiasi misura di sorveglianza che interferisca sulla sua realizzazione è illegittima così come stabilito dall'art. 19, comma 1, del Patto sui diritti civili e politici[58]. Diversamente, le limitazioni e le restrizioni sono ammissibili se si applicano alla libertà di espressione, intesa come libertà di esprimere un'opinione che si è previamente formata in modo libero ed autonomo, come indicato dall'art. 19, comma 2, del Patto sui diritti civili e politici [59].

A livello regionale, l'interpretazione e l'applicazione degli articoli che codificano le libertà in analisi non presentano particolari difformità rispetto al già menzionato articolo 19 del Patto sui diritti civili e politici [60]. Con specifico riferimento all'ingerenza delle misure di sorveglianza digitale sul godimento della libertà di opinione in relazione alla protezione della riservatezza, assume rilevanza il significato negativo della suddetta libertà come diritto a non essere identificati tra coloro che detengono un'opinione piuttosto che un'altra[61].

Recenti inchieste giornalistiche rilevano che l'ascesa di alcuni leader politici sia stata facilitata dalla messa in opera di vere e proprie "macchine *social*" volte all'acquisizione indebita di dati sensibili, anche se anonimi, della generalità degli utenti di piattaforme *online* di comunicazione. L'acquisizione di tali dati sembra volta principalmente a identificare – o meglio dire, a "profilare" – gli utenti a seconda delle loro opinioni e, quindi, a modulare, conformemente al "profilo" ottenuto, le informazioni da comunicare attraverso le suddette piattaforme così da influenzare la formazione delle opinioni politiche degli utenti[62].

In particolare, la Dichiarazione congiunta del maggio 2020 – adottata dai relatori speciali sulla libertà di opinione e di espressione delle Nazioni Unite e della Commissione

---

[58] Tra gli altri, v. M. O'FLAHERTY, *Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No 34*, in *Human Rights Law Rev.,* 2012, p. 627 ss.

[59] Ivi, p. 633 ss.

[60] Anche se la formulazione dell'articolo 10 della Convenzione europea e dei menzionati articoli delle altre Convenzioni differisce significativamente da quella dell'art. 19 del Patto sui diritti civili e politici, la libertà di opinione è ugualmente considerata la condizione preliminare delle altre libertà garantite dallo stesso articolo e gode di una protezione assoluta. Sul punto v. D. BYCHAWSKA-SINIARSKA, *A Handbook for Legal Practitioners*, Strasburgo, 2017, reperibile *online* al sito https://rm.coe.int. Inoltre, per la specifica questione dei limiti alla libertà di opinione ed espressione nei casi di incitamento all'odio, si rinvia a M. CASTELLANETA, *L'hate speech: da limite alla libertà di espressione a crimine contro l'umanità*, in G. VENTURINI, S. BARIATTI (a cura di), *Diritti individuali e giustizia internazionale, Liber Fausto Pocar*, Milano, 2009, p. 157 ss.; ID., *La Corte europea dei diritti umani e l'applicazione del principio dell'abuso del diritto nei casi di* hate speech, in *Dir. um. dir. int.*, 2017, p. 745 ss.

[61] Come già emergeva dai lavori preparatori dell'art. 19, comma 1, del Patto sui diritti civili e politici e dell'art. 10 della Convenzione europea, la violazione della libertà di opinione costituisce la deriva della democrazia. Sul punto v. Consiglio d'Europa, *European Commission on Human Rights-Preparatory Work on Article 10 of the European Convention on Human Rights*, Doc. DH (56) 15 del 17 agosto 1956, reperibile *online* al sito https://www.coe.int. Nel corso della storia non sono mancati esempi di ingerenze statali volte ad ottenere una "conversione politico-ideologica" dell'elettorato. Sul punto v. la comunicazione del Comitato dei diritti umani n. 878/1999, *Kang* c. *Corea*, UN Doc. CCPR/C/78/D/878/1999, osservazione del 16 luglio 2003, par. 7. Si veda in dottrina, per un commento generale su recenti avvenimenti, A. BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Riv. dir. int.*, 2019, p. 694 ss.

[62] M. GABANELLI, S. RAVIZZA, *Matteo Salvini e «La Bestia»: come catturare 4 milioni di fan sui social*, 20 ottobre 2019, reperibile *online* al sito https://www.corriere.it, dove con l'espressione "La Bestia" viene fatto riferimento alla suddetta "macchina *social*". Inoltre, v. R. ROTOLO, *Democrazia in Europa: quei social che isolano e paralizzano l'azione*, 5 settembre 2019; J. P. DARNIS, *Big Data: Cambridge Analytica, una svolta internazionale*, 21 marzo 2018, entrambi reperibili *online* al sito https://www.affarinternazionali.it.

interamericana, insieme all'OSCE[63] – richiama l'attenzione su situazioni preoccupanti come le minacce, gli attacchi violenti e le campagne diffamatorie contro i giornalisti da parte dei governi per ottenere l'appoggio dei media durante i periodi elettorali. Allo stesso modo, la predetta Dichiarazione fa specifico riferimento al problema della diffusione della disinformazione deliberata attraverso Internet e l'uso improprio delle piattaforme *social* da parte di attori statali e privati per cercare di sovvertire i processi elettorali[64].

Stando a queste informazioni, sembra plausibile affermare che le "macchine *social*" rappresentano un complesso sistema di sorveglianza digitale di massa suscettibile di costituire un'ingerenza ingiustificata ed arbitraria sulla tutela della riservatezza con un effetto domino sulla libertà assoluta di formarsi una opinione personale, autonoma ed incondizionata. Pertanto, non è da escludere che la messa in opera di "macchine *social*" potrebbe integrare una violazione della libertà di opinione in sede di accertamento della responsabilità internazionale di uno Stato che le ha utilizzate o che, comunque, non ha posto in essere le misure necessarie per evitarne l'utilizzo anche da parte di enti privati.

Recenti studi sull'ingerenza ingiustificata nella sfera della riservatezza (e sulle implicazioni che da tale ingerenza possono ricadere sul godimento effettivo della libertà di opinione) sono stati realizzati dal relatore speciale sulla libertà di opinione e di espressione. In tal senso, quest'ultimo ha dedicato particolare attenzione alla protezione dell'anonimato digitale ed alla libertà di accesso a tecniche di crittografia, mettendo in luce come la mancanza, o la percezione della mancanza, del rispetto della propria sfera personale possano interferire sul godimento effettivo del diritto di esprimersi liberamente[65].

Tuttavia, non è detto che un sistema di sorveglianza digitale che identifica gli utenti di una determinata piattaforma *online* costituisca una violazione della protezione dell'anonimato digitale, quale presupposto normativo del diritto al rispetto della riservatezza, congiuntamente o alternativamente, alla violazione della libertà di espressione. Infatti, a differenza della libertà di opinione, la tutela della riservatezza e della libertà di espressione possono subire limitazioni e restrizioni, come meglio preciseremo nel prossimo sottoparagrafo.

3.3. *L'obiettivo legittimo della sicurezza nazionale*

La valutazione della legittimità di misure di sorveglianza digitale che siano state adottate adducendo motivi di sicurezza nazionale dipende dal bilanciamento tra interessi contrapposti: da un lato, gli interessi particolari del singolo individuo o di un gruppo di

---

[63] *Declaración conjunta sobre libertad de expresión y elecciones en la era digital*, cit.

[64] Ivi, par. 1, spec. lettera *a*) e *b*); e, par. 2.

[65] Dobbiamo tener presente che attraverso specifiche tecniche che permettono di dissociare le informazioni riguardanti un utente dall'utente stesso, l'anonimato digitale ha aperto nuove opportunità di esprimersi liberamente, senza subire discriminazioni, censure, ovvero autocensure. Se da un lato le tecnologie informatiche contribuiscono alla realizzazione dell'autonomia e della dignità umana attraverso l'anonimato, allo stesso tempo, però, possono rendere gli strumenti di "anonimizzazione" sostanzialmente fallaci. Infatti, la raccolta e l'incrocio di metadati, insieme all'applicazione di tecniche statistiche e matematiche, permette di re-identificare l'effettivo detentore di informazioni, tenute originalmente anonime. Conseguentemente, attraverso l'adozione di misure di sorveglianza digitale, qualsiasi informazione, seppur anonima, potrebbe diventare personale, se combinata con altre informazioni rilevanti. Sul punto v. Consiglio dei diritti umani, *Report of the Special* Rapporteur *on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, UN Doc. A/HRC/29/32, del 22 maggio 2015, parr. 6-13 e parr. 14-28. Per una versione aggiornata di questo rapporto, v. *Research Paper 1/2018, Encryption and Anonymity Follow-up Report* del giugno 2018, reperibile *online* al sito https://www.ohchr.org.

individui con riguardo al godimento effettivo delle garanzie individuali; e, dall'altro, gli interessi collettivi che lo Stato rappresenta con riguardo alla necessità di far fronte a gravi minacce per la sicurezza.

La prassi dei meccanismi di tutela dei diritti umani mostra che tale processo di bilanciamento è basato su tre principi generali di diritto: il principio di legalità, il principio di necessità ed il principio di proporzionalità[66]. In virtù del principio di legalità, qualsiasi limitazione e restrizione di un diritto umano deve essere conforme alla legge statale; tali limitazioni devono inoltre essere formulate con sufficiente precisione in modo da evitare ingerenze discrezionali[67]. Dal canto suo, il principio di necessità comporta che l'ingerenza statale sia circoscritta a quanto strettamente indispensabile per la realizzazione di un obiettivo legittimo indicato negli strumenti internazionali di tutela, in modo coerente e compatibile con la protezione di altri diritti umani[68]. Infine, sulla base del principio di proporzionalità, le misure devono essere commisurate all'interesse da proteggere e devono essere congrue per raggiungere il risultato desiderato, utilizzando lo strumento meno invasivo tra quelli possibili e disponibili[69]. In nessun caso, comunque, le limitazioni e le restrizioni possono essere applicate o invocate in modo tale da compromettere l'essenza dei diritti in gioco[70].

In materia di sorveglianza digitale, assume particolare rilevanza l'interpretazione e la prassi applicativa che si è sviluppata, rispettivamente, nell'ambito del Comitato dei diritti umani e della Corte europea dei diritti umani.

Il Comitato dei diritti umani esercita diverse funzioni, tra cui quella di interpretare i diritti umani codificati dal Patto sui diritti civili e politici e di controllare il rispetto degli stessi da parte degli Stati. Nell'ambito della sua funzione interpretativa, assumono particolare rilevanza ai nostri fini i Commenti generali che il Comitato ha elaborato sul diritto alla riservatezza e sulla libertà di opinione e di espressione.

Il Commento generale n. 16 del 1988 sul diritto alla riservatezza può essere considerato il punto di partenza per ulteriori sviluppi normativi verso la tutela specifica di quest'ultimo diritto da "interferenze arbitrarie e illegittime"[71]. Già allora, nel contesto della sorveglianza (elettronica o di altro tipo), il Commento generale sottolineava esplicitamente che qualsiasi decisione volta a consentire interferenze con le comunicazioni dovesse essere presa "caso per caso" dall'autorità a tale scopo designata dalla normativa interna[72]. L'evoluzione delle modalità di ingerenza sulla riservatezza grazie all'impiego di una sempre più sofisticata

---

[66] Comitato dei diritti umani, *General Comment No. 27: Article 12 (1999),* UN Doc. CCPR/C/21/Rev.1/Add.9 del 2 novembre 1999, parr. 11-15. Inoltre, più recentemente con riguardo alle limitazioni e restrizioni realizzate attraverso misure di sorveglianza statale, si veda Consiglio dei diritti umani: *Report of the Special* Rapporteur *on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin*, UN Doc. A/HRC/13/37 del 28 dicembre 2009, par. 17; UN Doc. A/HCR/RES/28/16, cit.; UN Doc. A/HRC/29/32, cit.

[67] Comitato dei diritti umani, *General Comment No. 27*, cit., par. 12.

[68] *Ivi*, par. 14.

[69] *Ivi*, par. 15.

[70] Si veda sul punto, Comitato dei diritti umani, *General Comment No. 31 (80), The Nature of the General Legal Obligation Imposed on States Parties to the Covenant,* UN Doc. CCPR/C/21/rev.1/Add. 13 del 26 marzo 2004, par. 6.

[71] Comitato dei diritti umani, *General Comment No. 16: Article 17 (Right to Privacy),* cit., par. 4.

[72] *Ivi*, par. 8.

tecnologia digitale di sorveglianza di massa, oltre che di tipo mirato, ha aperto la discussione sull'opportunità di rivedere tale Commento in chiave contemporanea[73].

Per quanto concerne il Commento generale n. 34 del 2011 sulla libertà di opinione e di espressione, quest'ultimo costituisce una versione aggiornata di un precedente Commento generale, anch'esso del 1988[74]. Il Commento del 2011 dedica specifica attenzione al fenomeno di Internet e sottolinea l'obbligo generale degli Stati di garantirne il libero accesso ed utilizzo[75]. Inoltre, con riguardo alla legittimità delle restrizioni motivate da obbiettivi di sicurezza nazionale, richiama l'art. 19, comma 3, del Patto sui diritti civili e politici[76] ed invita gli Stati ad applicare le stesse in modo mirato così da evitare interferenze indiscriminate[77].

Nell'ambito della funzione di controllo che il Comitato dei diritti umani esercita, principalmente, a seguito della presentazione di comunicazioni individuali e di rapporti periodici degli Stati, lo stesso ha ribadito più volte il rispetto dei menzionati principi tenendo conto delle specifiche circostanze di ogni situazione[78].

Tra le osservazioni conclusive più recenti, il Comitato dei diritti umani, nell'analizzare le moderne tecniche di sorveglianza digitale di massa, ha adottato una interpretazione estensiva dell'applicabilità degli standards di condotta già elaborati in relazione alle misure di sorveglianza di tipo mirato a quelle di massa. In particolare, in occasione del rapporto periodico della Bielorussia, il Comitato ha reiterato l'obbligo a carico dello Stato di rispettare i diritti tutelati dal Patto sui diritti civili e politici nel contesto di operazioni di sorveglianza digitale, siano esse di tipo mirato che di massa, volte a migliorare la sicurezza nazionale. A tal proposito, viene fatto un riferimento esplicito al "triplice test di legittimità", conformemente ai principi di legalità, proporzionalità e necessità[79].

Passando al livello regionale, secondo la consolidata giurisprudenza della Corte europea dei diritti umani[80], il requisito della "previsione per legge", cui è subordinata la liceità

---

[73] Sul punto v. Consiglio dei diritti umani, UN Doc. A/HRC/13/37, cit., par. 19. Non va dimenticato che il relatore speciale sul diritto alla riservatezza, come già menzionato, dal 2015 dedica specifica attenzione a tale diritto nella prospettiva contemporanea dell'era digitale, ampliando la valutazione di "interferenze arbitrarie e illegittime" in modo conforme al "triplice test di legittimità". V., tra i più recenti, Consiglio dei diritti umani, UN Doc. A/HCR/RES/40/63, cit., parr. 26-45.

[74] Revisione della versione del 1988. Comitato dei diritti umani, *General Comment No. 34: Article 19 (Freedoms of Opinion and Expression)*, UN Doc. CCPR/c/GC/34 del 11 settembre 2011.

[75] *Ivi*, parr. 12, 15, 39 e 43-44.

[76] *Ivi*, parr. 21, 29, 30, 37 ss.

[77] Nello specifico, il Commento del 2011 invita gli Stati a criminalizzare tutte quelle attività considerate attinenti e/o connesse al terrorismo, come l'incoraggiamento o la sua glorificazione (ivi, par. 46).

[78] Nel caso di comunicazioni individuali, il Comitato si è trovato ad analizzare soprattutto casi di sorveglianza di tipo mirato, v. Comitato dei diritti umani: *Van Hulst* c. *Olanda*, *Communication No.* 903/1999, *Views* del 15 novembre 2004, UN Doc. CCPR/C/82/D/903/1999, par. 7.3; *Toonen* c. *Australia*, *Communication No.* 488/1992, *Views* del 31 marzo 1994, UN Doc. CCPR/C/50/D/488/1992, par. 8.3. Per i rapporti periodici, si veda il menzionato caso italiano, *supra* par. 3.1.

[79] Comitato dei diritti umani, *Concluding Observations: Belarus*, U.N. Doc. CCPR/C/BLR/CO/5 del 22 novembre 2018, parr. 43-44. Allo stesso modo, con il fine di sottolineare la coerenza delle osservazioni conclusive del Comitato rese con riguardo alla legittimità di misure di sorveglianza adottate da Stati con sistemi giuridici molto diversi tra loro, si veda anche, ID., *Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, U.N. Doc. CCPR/C/GBR/CO/7 del 27 agosto 2014, par. 24.

[80] Sul punto v. Consiglio d'Europa, *Thematic factsheet. Platform to Promote the Protection of Journalism and Safety of Journalists*, agosto 2017, reperibile *online* al sito https://www.coe.int. Per una rassegna della giurisprudenza rilevante, v., tra le schede informative del Consiglio d'Europa, *New Technologies,* ottobre 2019; ID., *Mass Surveillance*, agosto 2017; ID., *National Security and European Case-law*, 2013, disponibili *online* su https://www.echr.coe.int. Si precisa, inoltre, che la Corte europea e la Corte di Giustizia dell'Unione europea

di ogni ipotesi di restrizione di un diritto umano di natura relativa, comporta la necessità di individuare, nell'ordinamento nazionale, uno specifico riferimento normativo a tale restrizione[81]. Inoltre, tale riferimento deve essere accessibile per l'interessato in modo da consentire di prevedere ragionevolmente la restrizione del godimento del diritto in conseguenza del proprio comportamento[82].

Con riguardo ai requisiti della proporzionalità e della "necessità in una società democratica", la Corte ha seguito un'interpretazione restrittiva. In proposito, può essere richiamato il caso *Szabó e Vissy c. Ungheria* del 2016, in cui la stessa Corte ha accertato la contrarietà alla Convenzione europea della legge ungherese in materia di antiterrorismo per violazione del diritto alla riservatezza dei due ricorrenti[83]. Nello specifico, il caso riguardava due soggetti che lamentavano di essere stati sottoposti a misure di sorveglianza digitale in quanto membri di un'organizzazione no-profit che svolgeva attività di critica nei confronti del governo ungherese. La Corte, nel valutare la legittimità dell'obiettivo della lotta al terrorismo così come perseguito dalla legge ungherese, ha messo in luce due principali profili inerenti al significato della "stretta necessità" dell'ingerenza statale sulla sfera personale.

Sotto il primo profilo, la Corte ha ritenuto che l'adozione di misure di sorveglianza, anche quelle realizzate mediante sofisticate tecnologie digitali, debba essere "strettamente necessaria" per la salvaguardia delle istituzioni democratiche. Sotto il secondo profilo, ha precisato che le stesse devono essere "strettamente necessarie" e congrue al conseguimento di informazioni di fondamentale importanza per il buon esito dell'operazione di antiterrorismo. In qualsiasi altra situazione, come quella del caso *Szabó e Vissy*, la Corte ha ritenuto che la sorveglianza costituisca un abuso da parte delle autorità governative[84].

La giurisprudenza della Corte di Strasburgo, poi, ha posto particolare enfasi sulle garanzie che devono accompagnare le misure di sorveglianza digitale, come ad esempio, la previa autorizzazione da parte dell'autorità giudiziaria, ovvero da parte di organi di controllo indipendenti.

La previa autorizzazione non viene considerata dalla Corte come un requisito di per sé assoluto. In alcuni casi, infatti, è stato ritenuto sufficiente un controllo giudiziario posteriore all'adozione della misura, che sia idoneo a controbilanciare la carenza dell'autorizzazione[85]. L'importanza di un controllo giudiziario, previo o posteriore, alla realizzazione di misure di

---

tendono verso un dialogo costante volto ad evitare, per quanto possibile, discrasie nella prassi applicativa della tutela dei diritti in esame. Per un dettagliato esame sulla giurisprudenza della Corte di giustizia, v. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, cit., p. 18 ss.

[81] Per una accurata analisi della giurisprudenza della Corte europea in materia, v. L. SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, in L. PANELLA (a cura di), *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, cit., p. 107 ss.

[82] Tra le altre, v. Corte europea dei diritti umani: sentenza del 22 ottobre 2002, ricorso n. 47114/99, *Taylor-Sabori* c. *Regno Unito*, parr. 17-18; decisione di ammissibilità del 29 giugno 2006, ricorso n. 54934/00, *Weber e Saravia* c. *Germania*, parr. 93-94; sentenza del 13 febbraio 2018, ricorso n. 61064/10, *Ivashchenko* c. *Russia*, par. 59 ss.

[83] Sentenza della Corte europea dei diritti umani del 12 gennaio 2016, ricorso n. 37138/14, *Szabó e Vissy* c. *Ungheria*.

[84] Si veda sul punto, le sentenze della Corte europea dei diritti umani: *Szabó e Vissy* c. *Ungheria*, cit., parr. 71-73; *Weber e Saravia* c. *Germania*, cit., parr. 104-106.

[85] L'autorizzazione previa è un requisito imprescindibile per operazioni di tipo mirato nei confronti di giornalisti. Sul punto, v. Corte europea dei diritti umani: sentenza del 22 novembre 2012, ricorso n. 39315/06, *Telegraaf Media Nederland Landelijke Media B.V. e al.* c. *Olanda*, par. 101; ID., *Weber e Saravia* c. *Germania*, cit., par. 77.

sorveglianza digitale, è ribadita in più sentenze, con enfasi sull'importanza del rispetto dei principi fondamentali di uno stato di diritto[86].

Particolare attenzione è posta anche alla notifica delle misure di sorveglianza digitale, in quanto presupposto per il godimento del diritto ad un ricorso effettivo. Se l'interessato non è a conoscenza dell'esistenza di una tale ingerenza nei suoi confronti, questi non potrà difendersi contro eventuali abusi dei poteri di controllo da parte di autorità governative. Pertanto, la Corte ha sostenuto che la notifica debba essere eseguita nei confronti della persona interessata, non appena la situazione lo permetta e senza compromettere lo scopo della sorveglianza stessa[87].

A tal proposito, può essere richiamata la recente sentenza pronunciata dalla Corte di Strasburgo nel caso *Big Brother Watch e al.* c. *Regno Unito* del 2018[88]. Molto brevemente, i ricorrenti, 16 associazioni e giornalisti attivi nel campo della protezione delle libertà civili, lamentano l'utilizzo di un programma digitale d'intercettazione di massa – con ricerca, selezione, archiviazione e trasmissione dei dati raccolti dai servizi di comunicazione – da parte dei servizi segreti britannici in accordo con quelli americani[89].

L'interesse nell'analisi di questa sentenza deriva da alcune precisazioni che la Corte ha compiuto in merito alle garanzie che devono accompagnare le misure di sorveglianza di massa rispetto a quelle di tipo mirato[90]. Nel menzionato caso, la Corte ha affermato che l'assenza della previa autorizzazione e del controllo posteriore non sempre implicano che lo Stato stia agendo al di fuori dei "limiti di ciò che potrebbe essere ritenuto necessario in una società democratica". Tuttavia, non ha indicato quando la totale assenza del controllo da parte di un organismo indipendente potrebbe essere considerata legittima, rinviando ad una analisi caso per caso[91]. Inoltre, l'istituto della notifica è stato considerato nel caso *Big Brother Watch* come generalmente incompatibile con l'obiettivo stesso delle misure di sorveglianza di massa[92].

La natura indiscriminata delle misure di sorveglianza di massa sembra, dunque, aver portato la Corte di Strasburgo a dover (ri)considerare caso per caso le problematiche giuridiche collegate all'adozione di tali misure in assenza di specifiche garanzie procedurali. In caso di misure di sorveglianza di massa, quindi, assumono portata diversa le citate garanzie

---

[86] Cfr. Corte europea dei diritti dell'uomo: sentenza del 6 settembre 1979, ricorso n. 5029/71, *Klass e al.* c. *Germania*, parr. 56, 70 e 71; sentenza del 26 aprile 2007, ricorso n. 71525/2001, *Dumitru Popescu* c. *Romania (n. 2)*, par. 77; *Kennedy* c. *Regno Unito,* cit., parr. 184-191; sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Zakharov* c. *Russia*, par. 258. Per un'analisi della giurisprudenza relativa anche a casi di sorveglianza tra privati, si rinvia a L. SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, in L. PANELLA (a cura di), *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, cit., p. 110 ss.

[87] La sentenza della Corte europea dei diritti umani, *Szabo e Vissy* c. *Ungheria*, cit., par. 86.

[88] Corte europea dei diritti umani, *Big Brother Watch e al.* c. *Regno Unito*, cit.

[89] *Ibid.*

[90] La sentenza è complessa e sottopone tre specifiche questioni all'attenzione della Corte: in primo luogo, il generalizzato ed indiscriminato uso di tecniche digitali di intercettazione di informazioni e di acquisizione dati; in secondo luogo, il trasferimento dei dati acquisiti ad altri governi; e, infine, la problematica della richiesta ai fornitori di servizi di trasferire alle autorità governative i dati sensibili dei propri clienti.

[91] Sentenza della Corte europea dei diritti umani, *Big Brother Watch e al.* c. *Regno Unito*, cit., parr. 318-320; par. 338 ss. e par. 381. L'importanza di questo requisito non deve essere trascurata. In tal senso ricordiamo che il Comitato dei diritti umani ha recentemente invitato l'Italia ed altri a rivedere la normativa interna nella parte in cui consente alle autorità governative di condurre attività di monitoraggio senza previa autorizzazione giudiziaria. Sul punto v. *supra*, par. 3.1.

[92] Sentenza della Corte europea dei diritti umani, *Big Brother Watch e al.* c. *Regno Unito*, cit., par. 280 e parr. 316-317.

(in tema di controllo giurisdizionale e notifica delle misure) che sono invece sempre richieste a fronte di misure di sorveglianza mirata.

A conferma di quanto analizzato, tra le sentenze più recenti, il "triplice test di legittimità" viene rigorosamente ripreso nella già menzionata sentenza relativa al caso *P.N.* c. *Germania*[93]. La Corte di Strasburgo considera, infatti, che l'ingerenza statale della polizia tedesca nella sfera privata di individui che hanno determinati precedenti penali è prevista dalla legge nazionale[94] e persegue l'obiettivo legittimo della lotta preventiva alla criminalità[95]. Infine, la predetta Corte sottolinea che la sorveglianza digitale mediante la raccolta di dati utili per future indagini costituisce una interferenza necessaria e proporzionata tra l'esigenza di tutelare l'interesse pubblico alla prevenzione della criminalità e la limitazione del godimento della vita privata di soggetti già considerati responsabili di condotte criminose[96].

4. *Recenti sviluppi volti ad incentivare comportamenti responsabili da parte degli Stati*

Recenti sviluppi a livello internazionale, anche se di *soft law*, assumono specifica rilevanza sotto il profilo della responsabilità internazionale dello Stato per la conduzione di operazioni di sorveglianza digitale.

Nel 2004 l'Assemblea generale delle Nazioni Unite ha istituito un gruppo di esperti governativi (d'ora in avanti, secondo l'acronimo inglese, «GGE») con l'obiettivo di studiare l'impatto degli sviluppi delle tecnologie dell'informazione e della comunicazione nel contesto della sicurezza internazionale[97]. In particolare, l'obiettivo principale del GGE è quello di elaborare un modello di comportamento responsabile degli Stati in conformità con il principio di sovranità e giurisdizione statale e nel rispetto degli obblighi internazionali esistenti, con particolare enfasi sul rispetto dei fini e principi della Carta delle Nazioni Unite e dei diritti umani e delle libertà fondamentali.

Tale modello di comportamento responsabile include l'adozione di misure di rafforzamento della fiducia tra gli Stati sull'utilizzo di tali tecnologie digitali e suggerisce l'adozione di canali di comunicazione tra gli Stati per la gestione di tensioni e crisi internazionali a livello bilaterale, regionale e multilaterale[98]. Tuttavia, dal 2004 ad oggi, solo due relazioni finali del GGE sono state adottate per *consensus*[99].

L'evidente necessità di svolgere ulteriori studi e di superare i dissensi tra gli Stati, ha spinto l'Assemblea generale nel dicembre del 2018 a istituire, anche un gruppo di lavoro aperto a tutti gli Stati ed attori non-statali, rispettivamente per il periodo 2019-2021 e 2019-2020[100]. La situazione attuale non sembra poter dare risultati concreti a breve termine, anche

---

[93] Sentenza della Corte europea dei diritti umani, *P.N.* c. *Germania*, cit. Sul punto v. *supra*, par. 3.1.
[94] *Ivi*, par. 61 ss.
[95] *Ivi*, par. 68.
[96] *Ivi*, par. 69 ss.
[97] Assemblea generale: UN Doc. A/RES/58/32 del 8 dicembre 2003; A/RES/60/54 del 6 gennaio 2006; A/RES/66/24 del 13 dicembre 2011; A/RES/68/243 del 9 gennaio 2014; A/RES/70/237 del 30 dicembre 2015; A/RES/73/27 del 11 dicembre 2015; A/RES/73/266 del 2 gennaio 2019.
[98] Si pensi, ad esempio, all'Organizzazione per la cooperazione e la sicurezza in Europa ed il Forum Regionale dell'ASEAN.
[99] Cfr., i due rapporti del GGE sui quali è stato raggiunto un consenso: UN. Doc. /68/98 del 24 giugno 2013; UN Doc. A/70/174 del 22 luglio 2015. Gli incontri previsti per il 2019-2021 sono attualmente in corso.
[100] Assemblea generale, UN Doc. A/RES/73/266, cit., parr. 1-3.

se non deve essere trascurata l'importanza del ruolo dell'Assemblea generale nell'aver avviato questo processo di elaborazione di un modello di comportamento responsabile dello Stato, anche con il fine di tutelare i diritti umani e le libertà fondamentali della popolazione sottoposta alla loro rispettiva giurisdizione.

A questo, inoltre, deve aggiungersi il prezioso contributo di altri organismi istituiti dell'Assemblea generale. In particolare, nel maggio 2019 il relatore speciale sulla libertà di opinione e di espressione del Consiglio ONU sui diritti umani ha elaborato per la prima volta un rapporto specificamente dedicato a sorveglianza e diritti umani[101], in cui si sofferma sulla descrizione di alcune delle tecnologie di sorveglianza digitale più sofisticate prodotte e commercializzate dall'industria privata, con particolare attenzione sul grado di intensità degli effetti negativi che derivano dall'utilizzo delle stesse da parte degli Stati[102].

Nello specifico, il rapporto in questione contiene due proposte innovative. Da un lato, il relatore speciale promuove l'iniziativa di istituire un gruppo di lavoro all'interno del Consiglio dei diritti umani con lo scopo di realizzare uno studio delle misure di sorveglianza nazionali ed il loro impatto sulla tutela internazionale dei diritti umani e delle libertà fondamentali. In alternativa al gruppo di lavoro, propone la creazione di una *task force* interdisciplinare, oppure l'adozione di un piano d'azione specifico per far fronte agli effetti negativi della sorveglianza digitale[103]. Dall'altro lato, il relatore speciale invita gli Stati ad imporre un'immediata moratoria sull'utilizzo, vendita ed esportazione degli strumenti di sorveglianza digitale di tipo mirato fino a che non siano messe in atto rigorose garanzie in materia di diritti umani[104]. Dunque, sembra essere stata messa in discussione la presunzione di liceità delle misure di sorveglianza.

Questa nuova tendenza verso l'elaborazione di modelli di comportamento responsabile dello Stato e l'iniziativa di uno studio specifico per le misure nazionali di sorveglianza sembrano, dunque, aprire la strada verso sviluppi normativi in un contesto di cooperazione internazionale nel ciberspazio. Sotto il profilo della responsabilità internazionale dello Stato, tali sviluppi potranno essere utili per capire quando la condotta dello Stato è internazionalmente illecita, incluso in termini di violazione dei diritti umani e delle libertà fondamentali.

5. *Considerazioni conclusive*

Dall'indagine svolta risulta che le operazioni di sorveglianza digitale adottate dagli Stati per migliorare la sicurezza nazionale vengono, in linea di principio, ritenute lecite nell'ordinamento internazionale. Tuttavia, le misure in questione sono suscettibili di produrre effetti negativi soprattutto nel contesto della tutela dei diritti umani e delle libertà fondamentali.

Nel corso dell'indagine sono state evidenziate le difficoltà che emergono quando si cerca di accertare in quali casi tali effetti costituiscono una violazione degli obblighi di

[101] Il relatore speciale presta attenzione specifica alle misure di sorveglianza di tipo mirato, con particolare attenzione al comportamento degli Stati in rispetto all'utilizzo delle stesse. V. Consiglio dei diritti umani, *Surveillance and Human Rights*, UN Doc. A/HRC/41/35, cit.
[102] *Ivi*, parr. 7-14.
[103] *Ivi*, par. 65.
[104] *Ivi*, par. 66 (*a*).

condotta a carico degli Stati. Questo deriva soprattutto dal fatto che l'esercizio della sovranità nel ciberspazio presenta aspetti peculiari di intrinseca rilevanza internazionale che, però, non sono disciplinati da strumenti specifici a carattere multilaterale.

In particolare, per quanto riguarda la responsabilità per violazione di diritti umani, ci siamo soffermati sui possibili effetti negativi che legislazioni nazionali e prassi statali in materia di sorveglianza digitale possono produrre sul godimento di due diritti che maggiormente rischiano di essere lesi, ossia il diritto alla riservatezza e la libertà di opinione e di espressione.

Lo studio dei diritti presi in considerazione ha mostrato che l'interpretazione evolutiva che si è venuta ad affermare nel corso del tempo, anche in relazione all'esercizio di tali diritti *online*, ha ampliato i loro contenuti normativi ed incluso nuovi presupposti per il loro godimento effettivo, come la protezione dell'anonimato digitale.

Il passaggio successivo è stato quello di analizzare la legittimità di ingerenze statali su tali diritti, salvo il caso della libertà di opinione che è, invece, incondizionata e assoluta. La valutazione della legittimità di misure di sorveglianza per perseguire l'obiettivo della sicurezza nazionale mostra che per entrambe le tipologie di sorveglianza, si applicano i medesimi standard di condotta. Tuttavia, come mostrano le recenti sentenze dei casi *P.N.* c. *Germania* e *Big Brother Watch*, la Corte di Strasburgo ha seguito un approccio caso per caso, soprattutto in relazione alle garanzie procedurali che devono accompagnare le misure di sorveglianza digitale.

Recenti sviluppi normativi in seno alle Nazioni Unite sembrano aprire la strada a nuove forme di cooperazione internazionale nel ciberspazio verso la tutela di interessi comuni e dei diritti umani. Nello specifico, è apprezzabile il crescente sforzo della comunità internazionale, da un lato, verso l'elaborazione di un modello di comportamento responsabile dello Stato nel ciberspazio; e, dall'altro lato, verso la realizzazione di nuove iniziative a carattere internazionale volte a realizzare uno studio specifico ed esaustivo delle misure nazionali di sorveglianza digitale.

Sembra, dunque, opportuno riflettere su questi due recenti sviluppi e sul loro impatto sotto il profilo della responsabilità dello Stato.

In primo luogo, l'elaborazione di un modello di comportamento responsabile dello Stato nel ciberspazio sembra trovare la propria *ratio* nell'ambito più generale della progressiva realizzazione di strumenti di cooperazione multilaterale che sono volti a sensibilizzare gli Stati verso l'esercizio della cosiddetta "sovranità responsabile"[105]. In altre parole, l'affermazione del concetto di "sovranità come responsabilità" nell'ordinamento internazionale implica che la sovranità deve essere esercitata in modo "responsabile" da tutti gli Stati negli ambiti sottoposti alla loro giurisdizione nazionale, quindi, anche nel contesto della tutela dei diritti umani nel ciberspazio. A nostro avviso, ciò potrebbe contribuire a promuovere la cooperazione internazionale nel ciberspazio con lo scopo di predisporre specifici livelli di diligenza che indichino quando la conduzione di ciberoperazioni da parte degli Stati sia suscettibile di violare il diritto internazionale, in particolare i diritti umani e libertà fondamentali.

In secondo luogo, uno studio sulle misure nazionali di sorveglianza digitale, di tipo mirato e di massa, potrebbe risultare utile per arrivare ad una sistematizzazione delle stesse

[105] Si veda per una sintesi esaustiva di questo concetto, il discorso tenuto dall'allora Segretario generale delle Nazione Unite, Ban Ki-moon, in occasione dell'evento, *Responsible Sovereignty: International Cooperation for a Changed World*, 15 luglio 2008, reperibile *online* al sito www.un.org. Per un recente commento, si veda, C. FOCARELLI, *Diritto internazionale*, cit. p. 479 ss.

sulla base, ad esempio, di criteri di identificazione dei destinatari e di parametri di applicazione che siano condivisi dalla generalità degli Stati. Tale sistematizzazione aiuterebbe a modulare nuovi standard di condotta, e/o integrare quelli esistenti, da applicare all'una e/o all'altra nell'ambito del "triplice test di legittimità" al quale abbiamo fatto riferimento.

Questi sviluppi sembrano aprire la strada, dunque, verso una maggiore definizione dei contenuti degli obblighi di condotta a carico degli Stati in materia di sorveglianza digitale. Ciò potrebbe risultare utile come deterrente per evitare *a priori* la commissione di un illecito internazionale, in particolare, nel contesto della tutela dei diritti umani e delle libertà fondamentali; ma anche, *a posteriori,* per superare le menzionate criticità in sede di accertamento della responsabilità dello Stato.