Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2022, n. 3

EDITORIALE SCIENTIFICA
ES

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2022, n. 3

LA NORMALIZZAZIONE DELLA SORVEGLIANZA DI MASSA NELLA PRASSI GIURISPRUDENZIALE DELLE CORTI DI STRASBURGO E LUSSEMBURGO: VERSO IL CAMBIO DI PARADIGMA DEL RAPPORTO *PRIVACY V. SECURITY*

Michele Nino*

SOMMARIO: 1. Introduzione. – 2. Cenni storici: il caso *Datagate* e la condanna della sorveglianza di massa da parte delle Nazioni Unite e dell'Unione europea. – 3. La prima fase della prassi giurisprudenziale europea: l'illegittimità della sorveglianza di massa in base al diritto internazionale ed europeo. – 3.1. La Corte europea dei diritti dell'uomo: l'incompatibilità della sorveglianza in questione con la Convenzione europea dei diritti dell'uomo. – 3.1.1. La decisione adottata nel caso *Zakharov c. Russia*: la precisa indicazione dei rigorosi parametri tesi ad informare la sorveglianza dei dati personali. – 3.1.2. La sentenza resa nel caso *Szabó e Vissy c. Ungheria:* la conferma dei principi sanciti nella pronuncia *Zakharov* e la declinazione del requisito della necessità democratica *ex* articolo 8, par. 2, quale "stretta necessità". – 3.2. La Corte di giustizia dell'Unione europea: la contrarietà della conservazione massiva dei dati con il diritto dell'Unione europea: dalla sentenza *Digital Rights Ireland* alla decisione *Tele2 Sverige*, passando per le pronunce *Schrems I* e *II*. – 4. La seconda fase della prassi giurisprudenziale europea: verso la normalizzazione della sorveglianza di massa ed il cambio di paradigma del rapporto *privacy v. security*. – 4.1. La Corte di Strasburgo: la conformità della sorveglianza in blocco dei dati personali alla Convenzione europea dei diritti dell'uomo. – 4.1.1. La pronuncia *Big Brother Watch*: la legittimazione in base alla CEDU della intercettazione indifferenziata delle comunicazioni. – 4.1.2. La sentenza *Centrum för Rättvisa*: la conferma dei principi espressi nella decisione *Big Brother Watch*. – 4.1.3. La recente pronuncia *Ekimdzhiev:* un orientamento per molti versi neutro, a metà strada tra l'approccio espresso nelle sentenze *Zakharov* e *Szabó e Vissy* e quello affermato nelle decisioni *Big Brother Watch* e *Centrum för Rättvisa*. – 4.2. Il cambio di passo della Corte UE verso l'affermazione della compatibilità della conservazione generalizzata ed indiscriminata dei dati con il diritto dell'Unione europea: dalle decisioni *La Privacy International e La Quadrature du Net* fino ad arrivare alle recenti sentenze rese nei

Articolo sottoposto a doppio referaggio anonimo.

* Associato di Diritto internazionale, Università degli Studi di Salerno. Indirizzo e-mail: mnino@unisa.it.

1. Introduzione

Il presente lavoro ha ad oggetto l'analisi della legittimità della sorveglianza massiva dei dati personali in base al diritto internazionale ed europeo alla luce della prassi giurisprudenziale adottata negli ultimi anni tanto dalla Corte europea dei diritti dell'uomo quanto dalla Corte di giustizia dell'Unione europea.

La prima parte del contributo inquadra storicamente il fenomeno della sorveglianza in questione, analizzandone le ferme condanne nei principali *fora* internazionali. La seconda parte approfondisce la prima fase della prassi della Corte di Strasburgo e della Corte di Lussemburgo, le quali hanno sancito l'incompatibilità della raccolta indiscriminata e diffusa delle informazioni personali con la Convenzione europea dei diritti dell'uomo e la pertinente normativa UE in materia di privacy individuale. Nella terza parte dell'articolo viene esaminata la seconda fase della prassi in discussione, da cui si evince un evidente cambio di approccio da parte delle corti europee. Più precisamente in detta fase tali corti si sono pronunciate per l'ammissibilità della sorveglianza massiva dei dati personali, inaugurando un approccio basato sul cambio di paradigma tra privacy e sicurezza, maggiormente attento a soddisfare le esigenze securitarie rispetto a quelle fondate sulla tutela dei diritti umani e volto a normalizzare in definitiva questa forma di sorveglianza. Nella quarta ed ultima parte, dedicata alle conclusioni ed alle prospettive, viene auspicato che la Corte europea dei diritti dell'uomo e la Corte di giustizia dell'Unione europea tornino a confermare i principi espressi nella prima fase della loro giurisprudenza, così da riequilibrare il rapporto tra privacy e sicurezza e da evitare la normalizzazione della raccolta in blocco ed indifferenziata dei dati personali nella lotta al terrorismo ed alle gravi forme di criminalità organizzata.

2. Cenni storici: il caso *Datagate* e la condanna della sorveglianza di massa da parte delle Nazioni Unite e dell'Unione europea

La sorveglianza massiva dei dati personali per finalità di contrasto al terrorismo ed alla criminalità organizzata ha cominciato ad essere oggetto di un dibattito molto complesso e delicato nell'ambito dei principali *fora* internazionali successivamente alla scoperta del caso *Datagate*. Come è noto, nel giugno 2013 le rivelazioni di Edward Snowden, un ex dipendente della CIA, portarono alla luce dei media e della comunità internazionale l'esistenza del programma statunitense di sorveglianza elettronica, denominato PRISM[1]. Quest'ultimo, permettendo alle autorità di polizia e di *intelligence*

[1] The Guardian, G. GREENWALD, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, 6 giugno 2013, disponibile su www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-

USA – segnatamente la NSA (*National Security Agency*) e l'FBI (*Federal Bureau of Investigation*) – l'accesso diretto alle informazioni personali delle persone (ivi compresi i cittadini europei) che utilizzavano i principali *Internet Service Providers* americani[2], fu in grado di legittimare una sorveglianza indiscriminata e duratura dei dati in palese contrasto con la pertinente normativa internazionale ed europea in materia di privacy individuale[3].

In risposta allo scandalo suscitato dal caso in questione l'Assemblea generale delle Nazioni Unite adottò un'importante risoluzione intitolata "The right to privacy in the digital age", nella quale vennero sottoposte ad analisi due tipologie di sorveglianza potenzialmente coincidenti: quella illegittima e quella extraterritoriale[4]. La prima, ritenuta contraria ai principi di proporzionalità, necessità e finalità limitata, fu definita alla stregua di una chiara violazione del diritto alla vita privata e della libertà di espressione, in grado di pregiudicare le fondamenta di una società democratica[5]. Quanto, invece, alla sorveglianza extraterritoriale e massiva delle comunicazioni, l'Assemblea generale non adottò una posizione netta, in quanto, pur dichiarandosi preoccupata in ordine ai possibili abusi e lesioni dei diritti umani e delle libertà fondamentali che sarebbero potuti derivare dalla sua esecuzione[6], non la qualificò in maniera espressa quale evidente violazione dei diritti umani, come peraltro richiesto da Cuba e Venezuela[7]. Detta posizione fu frutto delle pressioni esercitate da alcuni Paesi, che, nella convinzione che la regolamentazione della privacy costituisse un elemento interno alle proprie politiche, rivendicarono la loro autonomia nella disciplina delle modalità di trasferimento e raccolta dei dati personali nel contesto digitale[8].

---

order; The Washington Post, *NSA Slides Explain the PRISM Data Collection Program*, 6 giugno 2013, disponibile su www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[2] Sul programma in questione, vedi: A. LUBIN, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, in *Chicago Journal of International Law*, 2018, n. 18, pp. 502-552, pp. 521-524.

[3] Vedi: Risoluzione del Parlamento europeo del 4 luglio 2013 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea, disponibile su eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013IP0322&from=IT; E. WATT, *The Right to Privacy and the Future of Mass Surveillance*, in *The International Journal of Human Rights*, 2017, n. 21, pp. 773-799.

[4] Risoluzione dell'Assemblea Generale delle Nazioni Unite del 18 dicembre 2013, *The Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167, considerando 8-11.

[5] Ivi, considerando 8; sul punto, vedi anche: F. DUBUISSON, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue trimestrielle des droits de l'homme*, 2016, n. 108, pp. 855-886, p. 856.

[6] UN Doc. A/RES/68/167, considerando 10; su tale atto, vedi: E. ROSSI, *Il diritto alla "privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in *Diritto comunitario e degli scambi internazionali*, 2014, n. 3, pp. 331-369, pp. 332-336.

[7] The Guardian, E. MACASKILL, J. BALL, *UN Surveillance Resolution Goes Ahead Despite Attempts to Dilute Language*, 21 novembre 2013, disponibile su www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language.

[8] The Guardian, D. RUSHE, *UN Advances Surveillance Resolution Reaffirming "Human Right to Privacy"*, disponibile su www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy; vedi anche: E. MACASKILL, J. BALL, *UN Surveillance Resolution Goes Ahead*, cit.; J. RIBEIRO, *UN Panel Passes Draft Resolution on Privacy Threats in the Digital Age*, disponibile su www.pcworld.com/article/448866/un-panel-passes-draft-resolution-on-privacy-threats-in-the-digital-age.html.

L'approccio espresso dall'Assemblea generale, sia pur embrionale e connotato da non poche lacune, ha rappresentato in ogni caso un meritorio tentativo, in quanto teso sia ad identificare e condannare per la prima volta alcune forme di sorveglianza delle comunicazioni potenzialmente pregiudizievoli dei diritti umani sia ad inaugurare un orientamento volto ad affermare il carattere imprescindibile della salvaguardia della vita privata nel contesto dell'evoluzione dell'era digitale e delle nuove tecnologie. Detto orientamento fu dapprima sviluppato dallo *Special Rapporteur* sulla promozione e protezione del diritto alla libertà di opinione ed associazione, Franck La Rue, nel suo rapporto del 2013[9] e fu di seguito rafforzato dalle Nazioni Unite attraverso il richiamo ai 13 principi sulla tutela dei diritti umani nell'ambito della sorveglianza elettronica, predisposti nel luglio 2013 da oltre 200 organizzazioni non governative[10].

Sulla stessa linea si pose il Parlamento europeo che ugualmente adottò una rilevante risoluzione, in cui, anche mediante il richiamo alla risoluzione dell'Assemblea generale, da un lato, condannò espressamente la vasta e sistemica raccolta indiscriminata e massiva dei dati personali di individui innocenti, da qualificarsi alla stregua di una ingerenza grave nei diritti fondamentali dei cittadini – idonea vuoi a produrre serie conseguenze negative sulla libertà di stampa, di pensiero e di parola e sulla libertà di riunione e associazione, vuoi a consentire attività illecite da parte dei servizi di *intelligence*[11]–; dall'altro, ravvisò nei programmi di sorveglianza massiva dei dati il consolidamento di un nuovo approccio basato su un regime di prevenzione informato a garanzie deboli ed inadeguate, non conformi allo Stato di diritto e non rispettose della presunzione di innocenza. Secondo il Parlamento europeo il sistema in discussione si poneva in conflitto con le basilari regole dello Stato di diritto, secondo cui le interferenze nei diritti fondamentali degli individui devono essere disciplinate dalla legge ed essere autorizzate da organi giurisdizionali indipendenti ed imparziali alla luce di un legittimo e ragionevole sospetto[12].

È in questo contesto – caratterizzato da forti critiche alla sorveglianza di massa per finalità di contrasto al terrorismo ed alla criminalità organizzata, manifestate sia dall'opinione pubblica mondiale sia dalle principali organizzazioni internazionali (universali e regionali) – che va inquadrata e compresa la prima fase della prassi

[9] 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.

[10] Principi internazionali in materia di applicazione dei diritti umani alla sorveglianza delle comunicazioni, 10 luglio 2013, disponibili su it.necessaryandproportionate.org/text. Siffatti principi costituiscono delle *guidelines* di particolare rilievo, in quanto tesi ad individuare parametri basilari in merito all'attuazione della sorveglianza delle comunicazioni nel contesto digitale, riproducendo di fatto i principi internazionali ed europei concernenti la salvaguardia della vita privata e dei dati personali (ovverosia: i principi di legalità, finalità limitata, adeguatezza, proporzionalità e trasparenza dei dati; la predisposizione di strumenti di controllo, indipendenti ed imparziali, con riguardo al trattamento dei dati; la previsione di misure atte ad assicurare l'integrità delle comunicazioni e la cooperazione internazionale tra Stati così come a punire la sorveglianza illegittima delle comunicazioni).

[11] Risoluzione del Parlamento europeo del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni, disponibile su eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52014IP0230&from=NL, par. 10.

[12] Ivi, par. 12.

giurisprudenziale adottata al riguardo tanto dalla Corte europea dei diritti dell'uomo quanto dalla Corte di giustizia dell'Unione europea, che sarà oggetto di studio nelle pagine che seguono.

3. La prima fase della prassi giurisprudenziale europea: l'illegittimità della sorveglianza di massa in base al diritto internazionale ed europeo

3.1. La Corte europea dei diritti dell'uomo: l'incompatibilità della sorveglianza in questione con la Convenzione europea dei diritti dell'uomo

3.1.1. La decisione adottata nel caso *Zakharov c. Russia*: la precisa indicazione dei rigorosi parametri tesi ad informare la sorveglianza dei dati personali

La prima sentenza adottata dalla Corte europea dei diritti dell'uomo successivamente al caso *Datagate*, nel clima di generale e comprensibile sfiducia a livello internazionale nei confronti della realizzazione della sorveglianza di massa, è quella resa nel 2015 nel caso *Zakharov c. Russia*[13]. Lo stesso, in particolare, traeva origine da un ricorso presentato alla Corte di Strasburgo da un cittadino russo, caporedattore di una casa editrice, che lamentava di aver subito una seria violazione del suo diritto alla vita privata, così come consacrato dalla Costituzione russa e dall'articolo 8 della CEDU. Ciò, in quanto la normativa russa (Ordine n. 70 del Ministero delle Comunicazioni), richiedendo agli operatori di rete mobile di installare apparecchiature che permettevano ai servizi di sicurezza nazionale di intercettare la totalità delle comunicazioni telefoniche senza preventiva autorizzazione giudiziaria, legittimava in buona sostanza una raccolta indifferenziata ed indiscriminata dei dati personali degli utenti[14].

Nel caso in esame la Corte ha apportato un notevole ed innovativo contributo alla ricostruzione del contenuto e delle garanzie sottese al diritto alla vita privata, tramite la identificazione dei requisiti di legittimità delle ingerenze in detto diritto nel sistema di Strasburgo. Come è noto, tali restrizioni sono giustificate in virtù dell'articolo 8 della CEDU solo laddove siano previste dalla legge e risultino necessarie in una società democratica per raggiungere determinati obiettivi legittimi[15].

Quanto al primo requisito, è stata posta in risalto l'esigenza che la normativa tesa a prevedere le misure di sorveglianza, non solo sia accessibile agli interessati e prevedibile nelle sue conseguenze, ma contempli anche idonee salvaguardie[16]. Con riferimento,

[13] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Zakharov c. Russia*.
[14] Ivi, par. 10.
[15] Gli obiettivi legittimi che giustificano le ingerenze nel diritto alla vita privata contemplati dall'articolo, 8, par. 2, della Convenzione europea dei diritti umani sono i seguenti: tutela della sicurezza nazionale e sicurezza pubblica; benessere economico del Paese; difesa dell'ordine; prevenzione dei reati; protezione della salute o della morale e salvaguardia dei diritti e delle libertà altrui.
[16] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., par. 237.

invece, al requisito della necessità democratica, è stato sancito – come da prassi – che, nell'attività di bilanciamento tra due interessi contrapposti (*sicurezza v. privacy*), le autorità nazionali dispongono di un particolare margine d'apprezzamento nella scelta dei mezzi per tutelare la sicurezza nazionale[17]. Tuttavia, in ragione del rischio che un regime di sorveglianza segreta predisposto per proteggere la sicurezza nazionale possa minare o addirittura distruggere la democrazia, è stata affermata la necessità che siffatto margine venga sottoposto a controllo da parte di organi competenti e che siano predisposte adeguate ed effettive garanzie contro gli abusi del potere governativo[18].

Più specificamente i giudici di Strasburgo hanno individuato in maniera analitica le garanzie minime che dovrebbero essere precisate dal legislatore nazionale nella disciplina delle misure segrete di sorveglianza, ovvero: la natura dei reati che possono giustificare un ordine di intercettazione; la definizione delle categorie di persone soggette a intercettazioni telefoniche; il limite alla durata delle intercettazioni telefoniche; la procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati ottenuti; le precauzioni da adottare nella comunicazione dei dati ad altri soggetti; e, infine, le circostanze in base alle quali le registrazioni possono o devono essere cancellate o distrutte[19].

A ciò si aggiunga che in merito alla notifica delle misure di sorveglianza, la Corte ha sancito un significativo principio volto a garantire l'azionabilità del diritto alla vita privata innanzi agli organi giudiziari statali, distinguendo a tal fine tre fasi: nelle prime due fasi – quella della prima adozione e quella della realizzazione di tali misure – la loro attuazione deve necessariamente essere posta in essere senza che l'individuo sottoposto a controllo ne sia a conoscenza[20]; nella terza fase – quella, cioè, in cui la sorveglianza venga a cessazione – la questione della successiva notifica delle misure di controllo è necessariamente collegata all'efficacia dei rimedi giurisdizionali e quindi all'esistenza di tutele effettive contro gli abusi dei poteri statali[21]. A tal riguardo, è stata ammessa la possibilità di notifica delle misure di sorveglianza all'interessato dalle stesse laddove ciò non pregiudichi gli obiettivi sottesi alla loro adozione[22]. In questo contesto, i giudici europei, sebbene abbiano consentito che in linea di massima vi sia un margine limitato per l'interessato di ricorrere alle autorità giurisdizionali competenti, hanno comunque riconosciuto che l'individuo, nel caso in cui venga informato delle misure adottate a sua insaputa, possa contestarne la legittimità *a posteriori*[23].

---

[17] Ivi, par. 232.

[18] Ivi; vedi anche: M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance*, in *Review of International, European and Comparative Law*, 2019, n. 17, pp. 84-103, p. 89.

[19] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., par. 231; sul punto, vedi: L. WOODS, *Zakharov v Russia: Mass Surveillance and the European Court of Human Rights*, disponibile su eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html.

[20] Corte europea dei diritti dell'uomo, Grande Camera, Zakharov, cit., par. 233.

[21] Ivi, par. 234.

[22] Ivi, par. 287; su questi profili, vedi: M. PALMISANO, *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and Their Application to Mass Surveillance in the United States and Russia*, in *Gonzaga Journal of International Law*, 2017, n. 20, pp. 75-99, p. 86.

[23] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., par. 234.

Infine, un altro parametro sviluppato dalla Corte è quello relativo alla natura ed ai presupposti dell'autorizzazione preventiva alla esecuzione delle misure di sorveglianza. Più esattamente, è stato statuito che siffatta autorizzazione debba essere concessa: 1. da un'autorità giudiziaria (o quantomeno un organo amministrativo indipendente dal potere esecutivo); 2. sulla base di un "reasonable suspicion" che la persona da sottoporre a controllo possa essere coinvolta in attività criminose, che possano altresì porre in pericolo la sicurezza nazionale[24]. L'affermazione della necessità di un controllo *ex ante* di un organo giurisdizionale e, soprattutto, l'introduzione nella propria giurisprudenza del nuovo criterio del ragionevole sospetto nel senso anzidetto, rappresentano un tentativo meritorio dei giudici europei di tutelare effettivamente le situazioni giuridiche soggettive contemplate dall'articolo 8 CEDU, così da evitare gli abusi dell'autorità governativa.

Nel caso di specie la Corte è giunta alla conclusione che la normativa russa regolante le intercettazioni di comunicazioni si poneva in contrasto con l'articolo 8 della CEDU, in quanto non prevedeva garanzie adeguate ed efficaci contro il rischio di abusi insiti in qualsiasi regime di sorveglianza segreta. Tale rischio era particolarmente elevato in un sistema ordinamentale, quale quello russo, in cui i servizi segreti e la polizia dispongono di un accesso diretto alle comunicazioni telefoniche di tutti gli utenti[25].

La pronuncia resa dalla Grande Camera nel caso *Zakharov* ha costituito una rilevante occasione per i giudici di Strasburgo al fine di: statuire rilevanti principi in materia di salvaguardia dei dati personali; chiarire e sviluppare alcuni parametri di protezione del diritto alla vita privata, definendo con maggiore precisione la portata applicativa dell'articolo 8 della CEDU a fronte dell'invasività delle misure statali di contrasto al crimine organizzato ed al terrorismo internazionale; ed esprimere una posizione univoca e garantista in materia, in linea con gli orientamenti espressi sia dalle Nazioni Unite che dall'Unione europea successivamente allo scandalo *Datagate*[26].

---

[24] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., par. 260; sul punto, vedi: V. RUSINOVA, *A European Perspective on Privacy and Mass Surveillance at the Crossroads*, 2019, disponibile su papers.ssrn.com/sol3/papers.cfm?abstract_id=3347711, pp. 1-22, p. 6; G. FORMICI, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo: da Zakharov a Big Brother Watch*, in *Federalismi.it*, 2020, n. 23, disponibile su www.federalismi.it/nv14/articolo-documento.cfm?Artid=43890, pp. 43-71, p. 54.

[25] In particolare sono state messe in rilievo le seguenti criticità del sistema normativo russo di intercettazione delle comunicazioni di telefonia mobile: mancata definizione delle circostanze in base alle quali le autorità pubbliche potevano utilizzare le misure di sorveglianza; assenza di previsione di garanzie sufficienti contro le interferenze arbitrarie; mancata indicazione della durata della conservazione dei dati; assenza di indicazioni circa le condizioni per l'archiviazione e la distruzione dei dati memorizzati; inadeguato controllo e mancata indipendenza delle autorità pubbliche; mancata prescrizione del diritto di notifica agli interessati dalle misure di controllo (Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., par. 302); vedi anche: Press Unit, Factsheet ECHR, *Mass Surveillance*, giugno 2022, disponibile su www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf, p. 3.

[26] Vedi: T. ACKERMANN, K. FENRICH, *Motion and Rest International Law's Responsiveness Towards Terrorism, Mass Surveillance, and Self-Defence*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 2017, n. 77, pp. 745-807, p. 784.

3.1.2. La sentenza resa nel caso *Szabó e Vissy c. Ungheria:* la conferma dei principi sanciti nella pronuncia *Zakharov* e la declinazione del requisito della necessità democratica *ex* articolo 8, par. 2, quale "stretta necessità"

In seguito alla decisione *Zakharov* la Corte ha reso nel 2016 un'altra importante sentenza nel caso *Szabó e Vissy c. Ungheria*, che traeva origine da un ricorso presentato da due componenti di un'organizzazione non governativa che esprimeva posizioni critiche nei confronti dell'operato del governo ungherese. Più precisamente, i ricorrenti lamentavano la circostanza che, nell'ambito delle attività di raccolta di dati di *intelligence*, la pertinente normativa nazionale[27] conferiva alla *Task Force* anti-terrorismo molteplici poteri, talmente ampi da legittimare una sorveglianza indiscriminata delle informazioni personali. In virtù di codesta normativa, infatti, detto organismo era legittimato a porre in essere una serie di attività molto invasive – ossia, perquisire segretamente abitazioni private; raccogliere ed aprire documenti, lettere e pacchi; controllare e registrare il contenuto del contenuto di comunicazioni elettroniche o informatiche – senza che fosse necessario a tal uopo il consenso delle persone interessate[28]. Inoltre l'autorizzazione giudiziaria era richiesta solo per l'attuazione della sorveglianza tesa ad indagare su taluni reati, e non per quella realizzata nell'ambito delle attività di *intelligence* finalizzate alla sicurezza nazionale (per cui era sufficiente unicamente l'approvazione governativa del Ministero della Giustizia)[29]. Infine, la legislazione in esame non imponeva alle autorità coinvolte alcun obbligo di distruzione del materiale di *intelligence* raccolto che potesse risultare irrilevante dopo la cessazione dell'attività di controllo[30].

In questa decisione la Corte ha confermato e rinsaldato per larga parte i principi espressi nella pronuncia *Zakharov*, sia pur differenziandosene in vari suoi aspetti. Innanzitutto la Grande Camera – consapevole del fatto che lo sviluppo e l'utilizzo delle nuove tecnologie, nonostante siano importanti in termini di efficacia della lotta al terrorismo ed alla criminalità organizzata, consentono ai governi nazionali di adottare misure di sorveglianza delle comunicazioni pregiudizievoli del diritto alla privacy individuale – ha invocato la necessità di una limitazione del margine di apprezzamento statale, introducendo a tal fine una nuova concezione del requisito della "necessità in una società democratica" contemplato dall'articolo 8, par. 2, della CEDU[31]. Più precisamente siffatto requisito va declinato alla stregua di una "stretta necessità" sotto due profili: una misura di sorveglianza segreta può essere ritenuta conforme alla Convenzione europea

[27] Art. 7/E, legge n. XXXIV del 1994 sulla polizia, come modificata dalla legge n. CCVII del 2011; sul punto, vedi: E. PÁSZTOR, *Secret Intelligence Gathering - A Low Threshold Still Too High to Reach. The Gap Between the Level of Privacy Protection in Europe and in Hungary After the Case of Szabó and Vissy v Hungary*, in *ELTE Law Journal*, 2017, n. 1, pp. 99-112, p. 105 ss.
[28] Corte europea dei diritti dell'uomo, Quarta Sezione, sentenza del 12 gennaio 2016, ricorso n. 37138/14, *Szabó e Vissy c. Ungheria*, parr. 8-9.
[29] Ivi, parr. 10-11.
[30] Ivi, par. 12.
[31] Ivi, parr. 68, 73; in relazione a tale profilo, vedi: T. ACKERMANN, K. FENRICH, *Motion and Rest International Law's Responsiveness Towards Terrorism*, cit., p. 787.

dei diritti dell'uomo solo se strettamente necessaria, come *considerazione generale*, per la salvaguardia delle istituzioni democratiche, e quale *considerazione particolare*, per l'ottenimento di informazioni fondamentali in una singola operazione di polizia[32]. I giudici di Strasburgo hanno poi sottolineato che questa innovativa interpretazione – ispirata ad un rigoroso approccio a tutela del diritto alla vita privata maggiormente garantista rispetto a quello espresso nel caso *Zakharov* – trova piena ed adeguata conferma negli orientamenti espressi dalla Corte di giustizia UE e dallo *Special Rapporteur* delle Nazioni Unite sulla promozione e protezione del diritto alla libertà di opinione e di espressione[33].

Nella decisione in discussione è stata tra l'altro sancita la necessità che, al fine di eseguire una sorveglianza delle comunicazioni, le autorità pubbliche dimostrino l'esistenza, non solo di un nesso tra le "persone o un gruppo di persone interessati" e la prevenzione di una minaccia terroristica, ma anche di un "sospetto individuale" riguardanti detti soggetti con riferimento a tale minaccia. In relazione a siffatto profilo, va peraltro detto che – come è stato anche osservato dal giudice Pinto de Albuquerque nella sua opinione concorrente – la Corte, accogliendo lo standard, indefinito e generico, del "sospetto individuale" rispetto a quello più garantista del "ragionevole sospetto" si è discostata da quanto precedentemente sancito nel caso *Zakharov* e ha, così, ridimensionato le tutele sottese al diritto alla vita privata *ex* articolo 8 della CEDU[34].

Peraltro, con rispetto alla necessità sia del riconoscimento di un diritto di notifica agli interessati dalla sorveglianza – notifica, questa, che risulta possibile a patto che non pregiudichi gli obiettivi di quest'ultima[35]– sia di un'autorizzazione preventiva alla sorveglianza stessa rilasciata da un'autorità giurisdizionale o quantomeno un organismo amministrativo indipendente da un apparato governativo[36], la Corte ha pienamente richiamato i parametri elaborati nel caso *Zakharov* rafforzando quanto ivi statuito[37].

Nel caso di specie i giudici di Strasburgo hanno stabilito che la legge ungherese si poneva in contrasto con l'articolo 8 della CEDU, in quanto legittimava una raccolta generalizzata di dati; non conteneva garanzie precise ed adeguate per evitare gli abusi governativi; non contemplava rimedi giurisdizionali idonei ed effettivi[38].

---

[32] Corte europea dei diritti dell'uomo, Quarta Sezione, Szabó e Vissy, cit., par. 73; sul punto, vedi: T. CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment*, in *European Law Blog*, 20 settembre 2018, disponibile su europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/; M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden*, cit., pp. 89-90; C. CINELLI, *Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani*, in *Ordine internazionale e diritti umani*, 2020, n. 3, pp. 588-608, pp. 603-604.

[33] Corte europea dei diritti dell'uomo, Quarta Sezione, *Szabó e Vissy*, cit., par. 73.

[34] Opinione concorrente del giudice Pinto de Albuquerque in Corte europea dei diritti dell'uomo, Quarta Sezione, *Szabó e Vissy*, cit., parr. 18-20, pp. 56-58; su questo aspetto, vedi: M. PALMISANO, *The Surveillance Cold War*, cit., p. 89.

[35] Corte europea dei diritti dell'uomo, Quarta Sezione, *Szabó e Vissy*, cit., par. 86.

[36] Ivi, par. 77.

[37] Vedi: T. CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance*, cit.

[38] Corte europea dei diritti dell'uomo, Quarta Sezione, *Szabó e Vissy*, cit., par. 89; sul punto, vedi: Press release issued by the Registrar of the Court, ECHR 014 del 12 gennaio 2016, *Hungarian Legislation on*

In conclusione, nelle sentenze *Zakharov* e *Szabó e Vissy*, mediante l'indicazione capillare dei requisiti atti a sovraintendere all'applicazione delle misure di sorveglianza delle comunicazioni e l'affermazione di principi tesi a circoscrivere in maniera significativa le ingerenze delle autorità statali in tale ambito – vale a dire, la restrizione del margine d'apprezzamento statale; la costruzione rigorosa dei requisiti di limitazione del diritto alla vita privata previsti dal regime di Strasburgo; la necessità di prevedere garanzie minime per gli interessati dalla sorveglianza; l'attribuzione a questi ultimi dei diritti di notifica e di contestazione *ex post* di una raccolta dei dati ritenuta illegittima; l'esigenza dell'autorizzazione giurisdizionale preventiva; e l'introduzione del criterio del sospetto o ragionevole o individuale –, la Corte ha sostanzialmente espresso con chiarezza meridiana l'incompatibilità della sorveglianza massiva, indiscriminata e diffusa, dei dati con l'articolo 8 della Convenzione europea dei diritti dell'uomo[39].

3.2. La Corte di giustizia dell'Unione europea: la contrarietà della conservazione massiva dei dati con il diritto dell'Unione europea: dalla sentenza *Digital Rights Ireland* alla decisione *Tele2 Sverige,* passando per le pronunce *Schrems I* e *II*

In linea con l'orientamento espresso dalla Corte europea dei diritti dell'uomo in questa prima fase si pone la prassi giurisprudenziale adottata dalla Corte di Giustizia dell'Unione europea, che ha riconosciuto la necessità della salvaguardia del diritto alla vita privata e dei dati personali nella lotta al terrorismo e alla criminalità organizzata, ed ha gradualmente escluso la legittimità della conservazione in blocco dei dati personali in base al diritto dell'Unione europea[40].

Secret Anti-Terrorist Surveillance Does not Have Sufficient Safeguards Against Abuse, p. 3; G. FORMICI, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo*, cit., p. 54.

[39] In tal senso, vedi anche: T. ACKERMANN, K. FENRICH, *Motion and Rest International Law's Responsiveness Towards Terrorism*, cit., pp. 786-790; M. BOHLANDER, *"The Global Panopticon": Mass Surveillance and Data Privacy Intrusion as a Crime Against Humanity?*, in M. BOHLANDER, M. BÖSE, O. LAGODNY, A. KLIP (eds.), *Justice Without Borders: Essays in Honour of Wolfgang Schomburg*, Leiden-Boston, 2018, pp. 73-102; M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden*, cit., pp. 89-90; V. RUSINOVA, *A European Perspective on Privacy and Mass Surveillance*, cit., p. 7.

[40] Sul punto, vedi: P. DE HERT, P.C. BOCOS, *Case of Roman Zakharov v. Russia: The Strasbourg Follow up to the Luxembourg Court's Schrems Judgment*, 23 dicembre 2015, disponibile su strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/; M.D. COLE, A. VANDENDRIESSCHE, *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in *European Data Protection Law Review*, 2016, n. 2, pp. 121-129; M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e "privacy": nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 2016, n. 23, pp. 1-26, disponibile su www.federalismi.it/nv14/articolo-documento.cfm?Artid=32831, p. 21; M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Rivista di diritto dei media*, 2018, n. 2, pp. 82-104, pp. 98-101; L. SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, in *Rivista di diritto dei media*, 2018 n. 2, pp. 132-145, p. 144; M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, 2021, n. 1, pp. 93-124, p. 94 ss.

La prima sentenza che la Corte di giustizia ha adottato al riguardo è quella resa nel caso *Digital Rights Ireland*, in cui il sistema di raccolta di dati predisposto dalla Direttiva n. 2006/24[41] (cd. direttiva sulla *data retention*) è stato considerato incompatibile con la normativa primaria UE sulla tutela delle informazioni personali[42]. In detta decisione, i giudici di Lussemburgo hanno annullato tale direttiva poiché la stessa, legittimando una conservazione indifferenziata delle telecomunicazioni con l'obiettivo di contrastare il terrorismo e la criminalità organizzata, risultava contraria ai principi europei di proporzionalità, necessità e finalità limitata dei dati ed era in grado di pregiudicare seriamente le garanzie sottese ai diritti alla vita privata ed alla protezione delle informazioni personali, contemplati dagli articoli 7 e 8 della Carta di Nizza[43]. Per quanto significativa nell'ambito di un quadro complessivo inteso a consolidare la salvaguardia della privacy individuale nell'ordinamento giuridico europeo dopo l'entrata in vigore del Trattato di Lisbona, la pronuncia in questione presentava tuttavia un limite di non poco rilievo, in quanto non conteneva una condanna espressa della raccolta indiscriminata delle informazioni personali e non identificava con chiarezza i principi sottesi alla attuazione della conservazione dei dati[44].

A colmare codeste lacune è intervenuta due anni dopo la sentenza del 2016 resa dalla Corte nel caso *Tele2 Sverige*[45], che concerneva peraltro l'interpretazione dell'articolo 15 della Direttiva n. 2002/58, che legittima gli Stati membri ad adottare misure legislative derogando ai principi sottesi alla tutela del diritto alla vita privata, allo scopo di salvaguardare la sicurezza nazionale e pubblica e di contrastare e prevenire reati[46]. In questa decisione, da un lato, è stata affermata l'illegittimità assoluta, in forza della

[41] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, del 15 marzo 2006 in GUUE L 105 del 13 aprile 2006, pp. 54-63.

[42] Corte di giustizia, Grande Sezione, sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri* e *Kärntner Landesregierung e altri*, cause riunite C-293/12 e C-594/12.

[43] Ivi, parr. 56-69; sulla sentenza, vedi: T. OJANEN, *Privacy Is More Than Just a Seven-Letter Word. The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance - Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*, in *European Constitutional Law Review*, 2014, pp. 528-541.

[44] Sul punto, vedi: F.-X. BRÉCHOT, *Clap de fin pour la conservation généralisée des données de connexion en Europe?: CJUE, gr.ch., 21 déc. 2016, aff. jtes C-203/15 et C-698/15, Tele2 Sverige et Watson e.a.*, in *Revue de l'Union européenne*, 2017, p. 178-187.

[45] Corte di giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele2 Sverige AB c. Post- och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e altri*, cause riunite C-203/15 e C-698/15.

[46] Art. 15, Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*, del 12 luglio 2002, in GUUE L 201 del 31 luglio 2002, pp. 37-47; sulla pronuncia, vedi: I. CAMERON, *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 2017, n. 54, pp. 1467-1495; S. PEYROU, *Arrêt «Tele2 Sverige»: l'interdiction du stockage de masse de données à caractère personnel réaffirmée par la Cour de justice de l'Union européenne*, in *Journal de droit européen*, 2017, n. 237 pp. 107-109, X. TRACOL, *The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level*, in *Computer Law & Security Review*, 2017, pp. 541-552.

normativa primaria e secondaria UE, della conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e di quelli relativi all'ubicazione della totalità degli abbonati e degli utenti iscritti riguardante tutti i mezzi di comunicazione elettronica per finalità di contrasto alle forme di criminalità grave. In effetti siffatta conservazione si poneva in palese contrasto con gli articoli 7, 8, 11 e 52 della Carta UE, e 15 della Direttiva n. 2002/58, eccedendo i limiti dello stretto necessario; determinando una interferenza grave nei diritti alla vita privata e alla protezione dei dati; non prevedendo nessuna differenziazione in ragione degli obiettivi conseguiti; non richiedendo alcun nesso tra i dati immagazzinati ed una minaccia per la sicurezza pubblica; non essendo limitata temporalmente e spazialmente; e non essendo circoscritta a determinate persone o gruppi di persone[47]. Dall'altro è stata sancita la compatibilità con il diritto UE della conservazione mirata dei dati personali, sempre che essa sia limitata allo stretto necessario "per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista"[48]. Più precisamente la normativa che prevede tale raccolta deve: essere chiara e precisa; contemplare garanzie sufficienti a tutela della privacy individuale e contro gli abusi dei poteri statali[49]; essere basata su una correlazione tra i dati personali conservati e le finalità da perseguire[50].

Nell'ambito di questo importante orientamento teso a rafforzare le garanzie sottese ai diritti alla vita privata nell'ordinamento giuridico europeo, confermato poi nel caso *Ministerio Fiscal* del 2018[51], vanno ricondotte anche le due pronunce adottate nei casi *Schrems I* (2015) e *Schrems II* (2020), in cui i giudici di Lussemburgo hanno annullato, rispettivamente, i regimi del *Safe Harbour* e del *Privacy Shield*, ovverosia le basi giuridiche che hanno permesso nei decenni scorsi la trasmissione dei dati tra UE e Stati Uniti[52]. In entrambi i casi i giudici di Lussemburgo hanno ritenuto siffatti sistemi non conformi alla rilevante normativa europea – in quanto volti a consentire una raccolta in blocco ed indifferenziata dei dati personali tra le due sponde dell'Atlantico – e hanno, tra l'altro, inquadrato la regolamentazione del trasferimento delle informazioni personali dall'UE ai Paesi terzi nell'ambito di un rigoroso rispetto dei diritti umani così come consacrati nella Carta di Nizza[53].

---

[47] Corte di giustizia, Grande Sezione, *Tele2 Sverige AB*, cit., parr. 97-107.
[48] Ivi, par. 108.
[49] Ivi, par. 109.
[50] Ivi, par. 110.
[51] Corte di giustizia, Grande Sezione, sentenza del 2 ottobre 2018, *Ministerio Fiscal*, causa C-207/16; sulla pronuncia, vedi: A. CAIOLA, *À la recherche de la juste pondération entre ingérence dans la vie privée et nécessité de lutte contre la criminalité*, in *Revue des affaires européennes*, 2018, n. 4, pp. 719-728.
[52] Sul punto, vedi: M. BASSINI, O. POLLICINO, *La Carta dei diritti fondamentali dell'Unione europea nel "reasoning" dei giudici di Lussemburgo*, in *Il diritto dell'informazione e dell'informatica*, 2015, nn. 4-5, pp. 741-777.
[53] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C-362/14; sentenza del 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, causa C-311/18; su tali decisioni, vedi: R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, 2016, pp. 289-307; E. URÍA GAVALÁN, *Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del*

4. La seconda fase della prassi giurisprudenziale europea: verso la normalizzazione della sorveglianza di massa ed il cambio di paradigma del rapporto *privacy v. security*

4.1. La Corte di Strasburgo: la conformità della sorveglianza in blocco dei dati personali alla Convenzione europea dei diritti dell'uomo

4.1.1. La pronuncia *Big Brother Watch*: la legittimazione in base alla CEDU della intercettazione indifferenziata delle comunicazioni

Successivamente alle decisioni analizzate in precedenza si è assistito ad un cambiamento sostanziale degli approcci tenuti dalla Corte di Strasburgo e dalla Corte UE, che hanno affermato viceversa la compatibilità della sorveglianza generalizzata con la CEDU e con il diritto dell'Unione europea.

L'espressione evidente di tale mutamento è rappresentata dalla sentenza del 2021 resa dalla Grande Camera della Corte di Strasburgo nel noto caso *Big Brother Watch e altri c. Regno Unito*[54], che ha non soltanto confermato, ma ha anche rafforzato, quanto già sancito dalla prima sezione nel 2018[55]. Il caso traeva origine da un ricorso presentato da talune organizzazioni a tutela dei diritti umani ed associazioni giornalistiche di categoria in seguito alle rivelazioni del caso *Datagate*, e teso a contestare la conformità alla Convenzione europea dei diritti dell'uomo della normativa britannica sulla sorveglianza e intercettazioni delle comunicazioni da parte dei servizi di *intelligence* e di sicurezza nazionali. Più esattamente sono stati avanzati dubbi di compatibilità con gli articoli 8 e

Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems, *Revista de derecho comunitario europeo*, 2016, n. 53, pp. 21-77; 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 *La rivista di diritto dei media*, 2018, pp. 64-81, p. 73; A. DEROUDILLE, *L'arrêt Schrems II, vers une résolution de l'équation transatlantique ?*, in *Revue de l'Union européenne*, 2021, n. 3, pp. 144-162.

[54] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorsi n. 58170/13 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*.

[55] Corte europea dei diritti dell'uomo, Prima Sezione, sentenza del 13 settembre 2018, ricorsi n. 58170/13 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*; sulla sentenza del 2018, vedi: Press release issued by the Registrar of the Court, ECHR 299 del 13 settembre 2018, *Some Aspects of UK Surveillance Regimes Violate Convention*; T. FALCHETTA, *Intelligence Sharing and the Right to Privacy After the European Court Judgment in Big Brother Watch v. UK*, in *EJIL:Talk! Blog of the European Journal of International Law*, 24 settembre 2018, disponibile su www.ejiltalk.org/intelligence-sharing-and-the-right-to-privacy-after-the-european-court-judgment-in-big-brother-watch-v-uk/; K. HUGHES, *Mass Surveillance and the European Court of Human Rights*, in *European Human Rights Law Review*, 2018, n. 6, pp. 589-599; M. TZANOU, *Big Brother Watch and Others v. The United Kingdom: A Victory of Human Rights over Modern Digital Surveillance?*, in *Verfassungsblog*, 18 settembre 2018, disponibile su verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/; B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance*, in *European Data Protection Law Review*, 2019, n. 5, pp. 252-261.

10 della CEDU di tre forme di comunicazione disposte da siffatta normativa: 1) l'intercettazione massiva delle comunicazioni; 2. la condivisione di materiale intercettato con agenzie di *intelligence* e governi stranieri; 3. l'ottenimento di informazioni personali da parte di fornitori di servizi di comunicazione.

Il *dictum* di particolare rilievo ed impatto contenuto nella pronuncia in esame, che si pone altresì in palese contrasto con l'orientamento espresso nei casi *Zakharov* e *Szabó e Vissy*, consiste nell'affermazione secondo cui l'intercettazione massiva di dati personali da parte dei servizi di *intelligence* non risulta essere di per sé contraria ai dettami previsti dalla Convenzione europea dei diritti dell'uomo, essendo tra l'altro la stessa configurabile quale strumento tecnologico di significativo rilievo al fine di contrastare il terrorismo e la criminalità organizzata nel contesto digitale[56]. Secondo la Corte, in particolare, la sorveglianza di massa è di vitale importanza nella identificazione di minacce alla sicurezza nazionale – anche alla luce del fatto che ulteriori ed alternative soluzioni non sarebbero in grado di sostituirla adeguatamente e di costituire un metodo parimenti valido a disposizione dei servizi di *intelligence*[57] – e non determina una ingerenza nella vita privata degli individui maggiore di quella realizzabile attraverso l'intercettazione mirata e dettagliata[58]. La valenza della sorveglianza in questione a fini preventivi e di contrasto a forme gravi di criminalità sarebbe confermata dalla circostanza che essa è spesso, se non prevalentemente, utilizzata per: raccogliere i dati di *intelligence* straniera; investigare preventivamente su attacchi cibernetici, di controspionaggio o attività terroristiche[59]; individuare nuove minacce da parte di soggetti conosciuti o non conosciuti; monitorare le comunicazioni internazionali, ovverosia, le comunicazioni di persone che si trovino al di fuori della giurisdizione territoriale di uno Stato, le quali potrebbero non essere controllate tramite differenti forme di sorveglianza[60]. Inoltre, tenendo in considerazione tanto la proliferazione delle minacce provenienti da attori internazionali che gli Stati sono chiamati ad affrontare in ambito digitale, quanto lo sviluppo di mezzi tecnologici che permette a tali *actors* di essere difficilmente identificabili, i giudici di Strasburgo hanno ricondotto la decisione di eseguire un regime di intercettazione di massa nell'ambito del margine di apprezzamento statale e quindi nel contesto di una valutazione discrezionale delle autorità governative nazionali[61].

Peraltro, allo scopo di contemperare le esigenze di sicurezza con quelle della tutela della vita privata e, dunque, di minimizzare i rischi di abusi da parte del potere statale derivanti dalla attuazione della intercettazione indifferenziata ed indiscriminata dei dati, i giudici di Strasburgo hanno sottoposto quest'ultima ad una serie di garanzie "end-to-

[56] Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 323.
[57] Ivi, parr. 166, 424.
[58] Ivi, par. 306.
[59] Ivi, parr. 322-345.
[60] Ivi, par. 344.
[61] Ivi, par. 340; su questi profili, vedi: J. SAJFERT, *The Big Brother Watch and Centrum för Rättvisa Judgments of the Grand Chamber of the European Court of Human Rights – The Altamont of Privacy?*, in *European Law Blog*, 8 giugno 2021, disponibile su europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/.

end", evidenziando la necessità che: 1. a livello nazionale, in ogni fase del processo vengano accertate la necessità e la proporzionalità delle misure adottate; 2. l'intercettazione in blocco sia sottoposta ad un'autorizzazione indipendente sin dall'inizio, dal momento, cioè, della definizione dell'oggetto e della portata dell'operazione; 3. l'operazione venga sottoposta a supervisione e revisione indipendente *ex post*[62]. Siffatte salvaguardie sono state poi maggiormente specificate mediante la definizione del contenuto della normativa nazionale intesa a disporre la sorveglianza indifferenziata ed attraverso l'integrazione ed aggiornamento delle cd. "sei garanzie" sancite in precedenza nel noto caso *Weber e Saravia*[63]. Purtroppo, però, la Corte non ha precisato al riguardo se le autorità statali debbano obbligatoriamente rispettare (o meno) i criteri evocati, limitandosi unicamente a stabilire in maniera generica che essi debbano essere complessivamente considerati nell'ambito di una "valutazione globale" della necessità e della proporzionalità della misura di sorveglianza[64]. Tale approccio è stato correttamente tacciato, da alcuni studiosi, di "feticismo procedurale", contestandosi alla Corte in buona sostanza di concentrarsi non sulla questione topica sottoposta alla sua attenzione – ossia la legittimità dei regimi di sorveglianza in base alla Convenzione europea dei diritti dell'uomo – ma piuttosto su garanzie procedurali dal contenuto e valore giuridico incerti[65].

Nel tentativo, poi, di delineare in dettaglio le garanzie in esame, la Grande Camera si è discostata ulteriormente dall'approccio tenuto nella sentenza *Zakharov* con riferimento

---

[62] Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 350; sul punto vedi: D. VOORHOOF, *Case Law, Strasbourg: Big Brother Watch v United Kingdom, Bulk Interception Regime Violated Articles 8 and 10 ECHR*, 9 giugno 2021, disponibile su biblio.ugent.be/publication/8711873/file/8711875.pdf.

[63] Vedi: Corte europea dei diritti dell'uomo, Terza Sezione, decisione del 29 giugno 2006, ricorso n. 54934/00, *Weber e Saravia c. Germania*, par. 95. In particolare, secondo la Corte, la normativa in questione deve precisare: 1. i motivi per i quali può essere autorizzata l'intercettazione di massa; 2. le circostanze in cui le comunicazioni di un soggetto possono essere intercettate; 3. la procedura da seguire per il rilascio dell'autorizzazione; 4. le procedure da seguire per la selezione, l'esame e l'utilizzo del materiale di intercettazione; 5. le cautele da adottare nella comunicazione del materiale ad altri soggetti; 6. i limiti alla durata dell'intercettazione, alla conservazione del materiale intercettato e le circostanze in cui tale materiale deve essere cancellato e distrutto; 7. le procedure e le modalità per il controllo da parte di un'autorità indipendente del rispetto delle garanzie indicate e i suoi poteri per far fronte al mancato rispetto di siffatte garanzie; 8. le procedure per l'esame indipendente *ex post* dell'osservanza di tali salvaguardie ed i poteri conferiti all'organo competente per svolgere codesto esame (Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 361).

[64] Ivi, par. 360; su detto profilo, vedi anche: M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa*, in *EJIL:Talk! Blog of the European Journal of International Law*, 26 maggio 2021, disponibile su www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/; M. ZALNIERIUTE, *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence*, in *EJIL:Talk! Blog of the European Journal of International Law*, 4 giugno 2021, disponibile su www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/; F. ZORZI GIUSTINIANI, *La normalizzazione della sorveglianza di massa nel contesto della CEDU e il Quarto Oxford Statement sulle tutele offerte dal diritto internazionale nel cyberspazio*, in *Cronache dal cyberspazio*, maggio-agosto 2021, pp. 1-5, disponibile su www.nomos-leattualitaneldiritto.it/wp-content/uploads/2021/10/CronachedalCyberspazio2_2021.pdf, p. 3.

[65] M. ZALNIERIUTE, *Procedural Fetishism and Mass Surveillance Under the ECHR. Big Brother Watch v. UK*, in *Verfassungsblog*, 2 giugno 2021, disponibile su verfassungsblog.de/big-b-v-uk/.

alla sussistenza del requisito del "ragionevole sospetto" per legittimare una raccolta in blocco delle informazioni personali. Più precisamente è stata esclusa l'applicabilità di codesto requisito a detta raccolta, avendo la stessa in linea di principio una finalità preventiva e non essendo tesa, d'altro canto, ad indagare su un obiettivo specifico o un reato identificabile[66].

In relazione al caso di specie sottoposto alla loro attenzione, i giudici europei hanno riscontrato la violazione dell'articolo 8 della CEDU, in quanto: il sistema di sorveglianza massiva disposto dalla normativa britannica non era stato autorizzato da un organismo indipendente dall'esecutivo ed era basato su presupposti assai vaghi; ed il regime per ottenere le comunicazioni dai fornitori di servizi di comunicazione non rispettava i parametri di protezione del diritto alla vita privata[67]. Viceversa, il meccanismo volto a disciplinare la condivisione di materiale intercettato con agenzie di *intelligence* e governi stranieri è stato ritenuto compatibile con tale articolo, alla luce della circostanza che risultava essere supportato da idonee salvaguardie[68].

La decisione *Big Brother Watch* è stata accolta positivamente da taluni come una "storica vittoria" della privacy e degli attivisti a tutela dei diritti umani e delle libertà fondamentali, anche e soprattutto in ragione delle conclusioni a cui è pervenuta in merito alla illegittimità della normativa britannica in base alla CEDU[69]. A ben vedere, peraltro, è vero esattamente il contrario: affermare la conformità alla Convenzione europea dei diritti dell'uomo della sorveglianza di massa – sempre che sia corredata da garanzie dal valore vincolante indefinito, confondendo il piano della utilità con quello della legittimità e richiamando contenuti e terminologie assai vaghi – equivale in definitiva a legittimare e normalizzare la intercettazione indiscriminata e duratura, sulla cui compatibilità alla luce dei principi europei di necessità, proporzionalità e finalità limitata dei dati è lecito avanzare molti dubbi[70].

Queste valutazioni critiche nei confronti della sentenza in discussione trovano conferma non solo nelle posizioni di numerosi studiosi[71], ma anche nella importante e

---

[66] Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 348; sul punto vedi: G. FORMICI, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo*, cit., p. 60. V. RUSINOVA, *A European Perspective on Privacy and Mass Surveillance*, cit., p. 12.

[67] Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 425.

[68] Sul punto vedi Press Unit, Factsheet ECHR, *Mass Surveillance*, cit., p. 5.

[69] PRIVACY INTERNATIONAL, *Human Rights Groups Win European Court of Human Rights Claim on UK Mass Surveillance Regime*, 25 maggio 2021, disponibile su www.privacyinternational.org/press-release/4522/human-rights-groups-win-european-court-human-rights-claim-uk-mass-surveillance; H. SIDDIQUE, *GCHQ's Mass Data Interception Violated Right to Privacy, Court Rules*, 25 maggio 2021, disponibile su www.theguardian.com/uk-news/2021/may/25/gchqs-mass-data-sharing-violated-right-to-privacy-court-rules.

[70] Vedi: M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments*, cit.

[71] Milanovic ha sostenuto che: "no - not a 'landmark victory' for privacy, but a grand, *definitive* normalization of mass surveillance by a virtually unanimous Grand Chamber for decades to come" (M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments*, cit.). Secondo Sajfert: "reading such statements about bulk interception eight years after the Snowden revelations leaves me, in the Court's own words, 'perplexed'" (J. SAJFERT, *The Big Brother Watch and Centrum för Rättvisa Judgments*, cit.). Con riferimento alla sentenza *Big Brother Watch* del 2018, le

articolata opinione (parzialmente concorrente e parzialmente dissenziente) del giudice Pinto de Albuquerque, che ha fortemente contestato i principi in essa contenuti, sottolineando la pericolosità dell'accettazione della intercettazione di massa, in quanto "l'utilità non è la stessa cosa della necessità e della proporzionalità in una società democratica"[72]. In particolare, il giudice ha sostenuto che la pronuncia, oltre ad utilizzare un linguaggio assai poco preciso[73], ha legittimato una pratica vietata dalla maggioranza dei Paesi europei e sostanzialmente inefficace nella prevenzione e nel contrasto alla minaccia terroristica[74], alterando così l'equilibro tra esigenze di protezione della vita privata e quelle securitarie[75]. In considerazione, dunque, del fatto che la decisione ha aperto "le porte ad un Grande Fratello elettronico in Europa", il giudice portoghese ha escluso di poter aderire all'idea di una nuova normalità voluta dalla maggioranza della Grande Camera[76].

Le opinioni parzialmente concordanti dei giudici Lemmens, Vehabović e Bošnjak si sono poste sostanzialmente sulla medesima lunghezza d'onda di detta opinione, sebbene abbiano espresso una posizione meno decisa. Tali giudici, difatti, sia pur accogliendo in principio la legittimità della sorveglianza di massa, hanno peraltro ammesso che la sentenza: non ha disposto alcuna chiara tutela sostanziale dell'individuo contro interferenze sproporzionate; avrebbe potuto conferire un peso notevolmente maggiore alla vita privata in generale e alla riservatezza della corrispondenza; e avrebbe dovuto richiedere l'autorizzazione giudiziaria per la realizzazione della sorveglianza di massa[77]. I giudici hanno altresì avvertito che "in order to avoid outright oppression and give itself

cui direttrici principali in merito alla politica della sorveglianza di massa sono state confermate dalla decisione del 2021, mentre Christakis ha evidenziato che "(i)n reality, the truth is that the European Court of Human Rights accepts the policy of mass surveillance" (T. CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance*, cit.), Lubin ha d'altro canto osservato che: "The bottom line of the judgment is this: not only has mass surveillance by governments become the new normal even in Europe … but this new normal has now received the Strasbourg Court's official stamp of approval!" (A. LUBIN, *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights*, 2 agosto 2018, disponibile su www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/). In questo orientamento vanno parimenti ricondotte le posizioni di altri autori: E. WATT, *The Right to Privacy and the Future of Mass Surveillance*, cit.; A. STIANO, *Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della Corte europea dei diritti dell'uomo*, in *Rivista di diritto internazionale*, 2020, n. 103, pp. 511-537; Ö.H. ÇINAR, *The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age*, in *The International Journal of Human Rights*, 2021, n. 25, pp. 26-51, pp. 43-44; F. DUBUISSON, *La Cour européenne des droits de l'homme face à la surveillance de masse (obs. sous Cour eur. dr. h., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021)*, in *Revue trimestrielle des droits de l'homme*, 2022, n. 129, pp. 123-141.

[72] Opinione parzialmente concorrente e parzialmente dissenziente del giudice Pinto de Albuquerque, in Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., par. 58, p. 196.
58.

[73] Ivi, par. 2, p. 167.

[74] Ivi, par. 11, p. 173.

[75] Ivi, par. 59, p. 196.

[76] Ivi, par. 60, p. 197; sul punto, vedi: E. WATT, *The Right to Privacy and the Future of Mass Surveillance*, cit.

[77] Opinione parzialmente concorrente dei giudici Lemmens, Vehabović e Bošnjak, in Corte europea dei diritti dell'uomo, Grande Camera, *Big Brother Watch*, cit., parr. 10, 14-24, pp. 158-163; sul punto, vedi: M. ZALNIERIUTE, *Procedural Fetishism and Mass Surveillance*, cit.

the varnish of legitimacy, there is an inherent danger that the State will utilise surveillance to ensure compliance and conformism", richiamando a tal riguardo un passaggio molto suggestivo del noto romanzo "1984" (*Nineteen Eighty-Four*) di George Orwell, in cui gli individui sono costretti a vivere con la consapevolezza che qualsiasi suono emesso o movimento posto in essere siano controllati dallo Stato "except in darkness"[78].

4.1.2. La sentenza *Centrum för Rättvisa*: la conferma dei principi espressi nella decisione *Big Brother Watch*

I *dicta* contenuti nella pronuncia *Big Brother Watch* sono stati pienamente confermati in una seconda pronuncia, adottata sempre dalla Grande Camera nel caso *Centrum för Rättvisa c. Svezia*[79], che ha in definitiva ribaltato le conclusioni raggiunte dalla terza sezione nel 2018[80]. Il caso in questione traeva origine da un ricorso presentato dalla organizzazione non governativa, Centrum för rättvisa, che lamentava che la normativa svedese sull'intelligenza dei segnali legittimava una sorveglianza di massa delle telecomunicazioni in contrasto con l'articolo 8 della Convenzione europea dei diritti dell'uomo[81].

La Corte ha ribadito e rafforzato i principi secondo cui: 1. l'intercettazione in blocco dei dati personali non risulta di per sé contraria ai dettami della CEDU e costituisce uno strumento vitale a disposizione delle autorità di *intelligence* e di contrasto al crimine[82]; 2. la scelta di darne attuazione, allo scopo di identificare e prevenire minacce contro la sicurezza nazionale o attacchi a fondamentali interessi nazionali, rientra nel margine d'apprezzamento delle autorità statali[83]; 3. l'intercettazione medesima deve sottostare al rispetto delle garanzie "end-to end" già evocate e declinate nel caso *Big Brother Watch*,

[78] Opinione parzialmente concorrente dei giudici Lemmens, Vehabović e Bošnjak, in Corte europea dei diritti dell'uomo, Grande Camera, Big Brother Watch, cit., par. 6, p. 157; sul punto vedi: D. VOORHOOF, *Case Law, Strasbourg: Big Brother Watch v United Kingdom*, cit.

[79] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorso n. 35252/08, *Centrum för Rättvisa c. Svezia*.

[80] Corte europea dei diritti dell'uomo, Terza Sezione, sentenza del 19 giugno 2018, ricorso n. 35252/08, *Centrum för Rättvisa c. Svezia*; su questa decisione, vedi: V. RUSINOVA, *A European Perspective on Privacy and Mass Surveillance*, cit.; M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden*, cit.; G. FORMICI, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo*, cit.

[81] Corte europea dei diritti dell'uomo, Grande Camera, *Centrum för Rättvisa*, cit., parr. 10-12. A tal proposito va precisato che l'intelligenza dei segnali consiste nell'intercettazione, elaborazione, analisi e raccolta dei dati attraverso i segnali elettronici. In Svezia la conservazione massiva di detti segnali rappresenta una delle forme di *intelligence* straniera ed è disciplinata dal *Signal Intelligence Act*, che consente ad un'autorità dipendente dal Ministero della Difesa ((*Försvarets radioanstalt* "FRA") di realizzare siffatta pratica tramite la intercettazione di massa (vedi: paras. 14, 17); per una ricostruzione di questa normativa, vedi: M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden*, cit., p. 91 ss.

[82] Corte europea dei diritti dell'uomo, Grande Camera, *Centrum för Rättvisa*, cit., par. 365.

[83] Ivi, par. 254.

perché non si traduca in un'attività lesiva dei diritti umani ad opera delle autorità di governo[84].

Nel caso di specie la Corte ha accertato che la normativa svedese di intercettazione di massa presentava tre lacune di non poco momento: non prevedeva una norma chiara sulla distruzione del materiale intercettato non contenente dati personali; non includeva una disposizione garantista che tenesse conto della protezione della privacy individuale, in caso di trasmissione di materiale di *intelligence* ad entità straniere; non contemplava un effettivo riesame *ex post* della sorveglianza delle comunicazioni[85]. Non contenendo, quindi, adeguate garanzie "end-to-end" idonee a salvaguardare il diritto alla vita privata, tale regime è stato ritenuto in contrasto con l'articolo 8 della CEDU[86].

Questa sentenza, che si inquadra nel discutibile orientamento inaugurato dalla Grande Camera nel caso *Big Brother Watch* teso ad affermare la normalizzazione della sorveglianza di massa[87], è stata parimenti criticata dal giudice Pinto de Albuquerque. Questi, nella sua opinione concorrente, oltre a confermare la sua visione sulla raccolta in blocco dei dati espressa in detto caso, ha contestato l'approccio tenuto dalla Corte dal punto di vista metodologico, tanto per non aver accertato la veridicità delle argomentazioni avanzate dal governo svedese, quanto per non aver valutato la prassi nazionale in materia di raccolta massiva delle informazioni personali[88]. Considerazioni negative nei confronti della pronuncia in discussione sono provenute anche da parte di alcuni autori, che hanno evidenziato la mancata attenzione rivolta dai giudici di Strasburgo alla pertinente prassi adottata dalle autorità giurisdizionali ed esecutive svedesi[89].

4.1.3. La recente pronuncia *Ekimdzhiev:* un orientamento per molti versi neutro, a metà strada tra l'approccio espresso nelle sentenze *Zakharov* e *Szabó e Vissy* e quello affermato nelle decisioni *Big Brother Watch* e *Centrum för Rättvisa*

Per completare il quadro relativo alla prassi giurisprudenziale della CEDU in tema di sorveglianza delle comunicazioni, appare opportuno fare riferimento alla recente sentenza adottata dalla Corte di Strasburgo nel gennaio 2022 nel caso *Ekimdzhiev e altri c.*

[84] Ivi, par. 264; sul punto, vedi: Press release issued by the Registrar of the Court, ECHR 164 del 25 maggio 2021, *Insufficient Safeguards in Bulk Signals-Intelligence Gathering Risked Arbitrariness and Abuse*, p. 1.
[85] Corte europea dei diritti dell'uomo, Grande Camera, Centrum för Rättvisa, cit., par. 369; sul punto, vedi: M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments*, cit.
[86] Corte europea dei diritti dell'uomo, Grande Camera, *Centrum för Rättvisa*, cit., parr. 373-374; su tale aspetto, vedi: D. VOORHOOF, *Case Law, Strasbourg: Big Brother Watch v United Kingdom*, cit.
[87] In questo senso, vedi: M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments*, cit.
[88] Opinione concorrente del giudice Pinto de Albuquerque, in Corte europea dei diritti dell'uomo, Grande Camera, *Centrum för Rättvisa*, cit., par. 1, p. 96.
[89] M. KLAMBERG, *Big Brother's Little, More Dangerous Brother. Centrum för Rättvisa v. Sweden*, in *Verfassungsblog*, 1° giugno 2021, disponibile su verfassungsblog.de/raettvisa/; F. ZORZI GIUSTINIANI, *La normalizzazione della sorveglianza di massa nel contesto della CEDU*, cit., p. 4.

Bulgaria, cercando soprattutto di capire in quale linea di orientamento essa vada inquadrata[90].

Il caso traeva origine da una serie di ricorsi presentati da due cittadini e due associazioni non governative bulgari, i quali sostenevano che la natura delle proprie attività li poneva a rischio sia di sorveglianza segreta sia di accesso ai dati delle loro comunicazioni da parte delle autorità nazionali in forza della normativa bulgara che autorizzava dette attività[91]. Pertanto i giudici di Strasburgo sono stati richiesti di accertare la compatibilità con l'articolo 8 della CEDU di due categorie di norme: quella regolante la sorveglianza segreta; quella disciplinante la raccolta delle informazioni personali da parte dei fornitori dei servizi di telecomunicazioni e l'accesso conseguente a siffatte informazioni ad opera delle autorità di *intelligence* e di polizia. A tal riguardo, è stata effettuata una valutazione per ciascuna di queste categorie con riferimento ai medesimi criteri: l'accessibilità della legge; le ragioni secondo cui è possibile consentire la sorveglianza segreta e l'accesso dei dati da parte delle autorità di contrasto al crimine; le regole sulla durata della raccolta e sui tempi di archiviazione ed utilizzazione dei dati da parte di dette autorità; le procedure di autorizzazione per la conservazione, l'accesso, l'esame, l'utilizzo, la comunicazione e la distruzione delle informazioni personali oggetto di sorveglianza; i meccanismi di controllo; i sistemi di notificazione degli interessati dalla raccolta; i rimedi a disposizione di questi ultimi[92].

A seguito di accertamenti particolarmente tecnici svolti relativamente a detti parametri, la Corte è giunta alla conclusione che entrambe le normative analizzate violavano l'articolo 8 della CEDU, in quanto non rispettavano il requisito della "qualità della legge" e realizzavano un'ingerenza nella vita privata dei soggetti sottoposti a controllo, che andava oltre ciò che era "necessario in una società democratica"[93].

Analizzando complessivamente la pronuncia in esame, è possibile ritenere che la stessa si situi a metà strada tra l'approccio garantista a tutela dei diritti umani espresso nelle decisioni *Zakharov* e *Szabó e Vissy* e quello più attento alle esigenze securitarie sancito nelle pronunce *Big Brother Watch* e *Centrum för Rättvisa*[94]. Da un canto, infatti, la sentenza *Ekimdzhiev* è riconducibile al primo approccio nella misura in cui non solo manifesta un atteggiamento critico nei confronti di un sistema, quale quello bulgaro, che potrebbe teoricamente legittimare un controllo generalizzato ed indifferenziato dei dati, ma prevede anche in dettaglio una serie di garanzie per porre freno agli abusi del potere esecutivo[95]. Dall'altro, siffatta sentenza è inquadrabile nel secondo approccio laddove

[90] Corte europea dei diritti dell'uomo, Quarta Sezione, sentenza dell'11 gennaio 2022, ricorso n. 70078/12, *Ekimdzhiev e altri c. Bulgaria*.
[91] Ivi, parr. 2-10.
[92] Ivi, parr. 296-359; 396-421.
[93] Ivi, parr. 358-359; 420-421; sul punto, vedi anche: Press release issued by the Registrar of the Court, ECHR 009 dell'11 gennaio 2022, *Flaws in Legal Safeguards and Oversight Procedures Around Secret Surveillance*.
[94] D. DIMITROVA, *Ekimdzhiev and Others v. Bulgaria: Secret Surveillance and Electronic Communications Surveillance Only With Adequate Safeguards, or Nothing New Under the Sun*, 2 marzo 2022, disponibile su strasbourgobservers.com/2022/03/02/ekimdzhiev-and-others-v-bulgaria-nothing-new-under-the-sun/.
[95] Ivi.

essa: non richiede coerenti garanzie con riguardo alla autorizzazione giudiziaria alla sorveglianza segreta; stabilisce che la richiesta del controllo da parte delle autorità di polizia e di *intelligence* alle autorità competenti in materia di terrorismo possa essere corredate da minori salvaguardie; non affronta né prende posizione circa la *vexata quaestio* della ammissibilità della conservazione massiva delle informazioni personali in base ai principi europei di necessità e proporzionalità[96].

D'altronde, cercando di cogliere ancor di più approfonditamente il senso di detta decisione alla luce della prassi della Corte di Strasburgo finora tratteggiata, va osservato che l'atteggiamento in essa espresso, se è vero che si caratterizza per un'apparente neutralità di fondo rispetto agli approcci menzionati; è parimenti vero che, nel momento in cui manifesta una certa riluttanza ad affrontare le questioni centrali concernenti la legittimità della intercettazione in blocco, esprime implicitamente la volontà di confermare e validare lo stato e l'orientamento attuale della prassi giurisprudenziale in discussione, che è al momento, come si è visto, tesa alla affermazione della normalizzazione della sorveglianza massiva dei dati personali.

4.2. Il cambio di passo della Corte UE verso l'affermazione della compatibilità della conservazione generalizzata ed indiscriminata dei dati con il diritto dell'Unione europea: dalle decisioni *La Privacy International e La Quadrature du Net* fino ad arrivare alle recenti sentenze rese nei casi *H.K. c. Prokuratuur* e *Commissioner of An Garda Síochána*

Un approccio per molti versi speculare a quello tenuto dalla Corte europea dei diritti dell'uomo nei casi *Big Brother Watch* e *Centrum för Rättvisa* è quello che dal 2020 sta esprimendo la Corte di giustizia UE attraverso l'adozione di talune decisioni che scaturiscono da una serie di questioni pregiudiziali sollevate da diverse autorità giurisdizionali nazionali, aventi ad oggetto l'interpretazione dell'articolo 15 della Direttiva n. 2002/58.

Innanzitutto vanno menzionate due pronunce rese rispettivamente nei casi *Privacy International* e *La Quadrature du Net*, particolarmente importanti poiché hanno dato l'avvio ad un cambio di passo della Corte di Lussemburgo rispetto alle posizioni garantiste a protezione dei diritti umani espresse in passato nelle sentenze *Tele2 Sverige*, *Ministerio Fiscal*, *Schrems I* e *II*[97].

Il primo caso traeva origine da un ricorso promosso innanzi all'*Investigatory Powers Tribunal* dalla organizzazione non governativa Privacy International contro il governo britannico, che riguardava la tematica della legittimità, in virtù della pertinente normativa europea, della conservazione ed utilizzo di massa delle informazioni personali ad opera delle agenzie di sicurezza e di *intelligence* del Regno Unito. Il secondo caso derivava da

[96] Ivi.
[97] Sul punto, vedi: M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, cit., p. 101 ss.

una serie di ricorsi presentati da alcune organizzazioni di categoria, francesi e belghe, contro i rispettivi governi nazionali innanzi alle autorità giurisdizionali dei loro Paesi, concernenti la compatibilità con il diritto UE delle legislazioni francesi e belghe, intese a disciplinare la raccolta, il trattamento e l'uso delle comunicazioni elettroniche e ad ammettere in definitiva una conservazione in blocco dei dati personali degli utenti dei servizi di comunicazione.

In questi due casi, allo scopo di valutare la legittimità della conservazione dei dati di traffico e di quelli relativi all'ubicazione, la Corte di giustizia ha individuato due criteri discretivi basati sulle finalità conseguite dalla conservazione medesima: la tutela della sicurezza pubblica e la salvaguardia della sicurezza nazionale.

Più precisamente, con riguardo alla prima finalità, è stata sancita l'incompatibilità con la pertinente normativa UE – articolo 15 della Direttiva n. 2002/58; articoli 7, 8 e 11 della Carta di Nizza – della raccolta generalizzata e indifferenziata dei dati posta in essere per conseguire la suddetta finalità. Ciò, in quanto siffatta raccolta eccede i limiti dello stretto necessario e risulta essere non giustificata in una società democratica, poiché non solo implica un accesso generale, indiscriminato e duraturo alla totalità delle informazioni personali in assenza di qualsivoglia nesso (anche indiretto o remoto) con l'obiettivo perseguito, ma comporta anche un'interferenza grave nei diritti contemplati dalle previsioni citate[98]. Peraltro, è stata affermata la conformità alla predetta normativa della conservazione preventiva e mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, sempre che la medesima sia circoscritta temporalmente e limitata allo stretto necessario quanto alle persone da sottoporre a controllo, agli strumenti di comunicazione utilizzati ed alle categorie dei dati da raccogliere[99].

Di converso, nel caso *La Quadrature du Net*, la Corte UE, con rispetto all'obiettivo della protezione della sicurezza nazionale, ha statuito che esso, interpretato alla luce dell'articolo 4, paragrafo 2, TUE, è di maggiore rilevanza rispetto a quello della salvaguardia della sicurezza pubblica ed è in grado di giustificare misure che implichino interferenze nei diritti fondamentali più gravi di quelle che potrebbero richiedere altri obiettivi[100]. Di conseguenza, nel caso in cui uno Stato si trovi a dover fronteggiare una minaccia grave, che sia "reale e attuale o prevedibile", l'articolo 15 della Direttiva n. 2002/58, letto alla luce della pertinente normativa primaria UE, non esclude che detto Stato possa adottare una misura legislativa che permetta alle autorità competenti di imporre ai fornitori di servizi di comunicazione elettronica una conservazione generalizzata ed indifferenziata dei dati, che coinvolga la totalità di detti utenti e che prescinda da un nesso tra gli stessi e la minaccia in questione[101].

[98] Corte di giustizia, Grande Sezione: sentenza del 6 ottobre 2020, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e altri*, causa C-623/17, parr. 78-82; sentenza del 6 ottobre 2020, *La Quadrature du Net e altri c. Premier ministre e altri*, cause riunite C-511/18, C-512/18 e C-520/18, parr. 141-144.
[99] Corte di giustizia, Grande Sezione, *La Quadrature du Net*, cit., par. 147.
[100] Ivi, par. 136.
[101] Ivi, par. 137.

I giudici di Lussemburgo nel caso *La Quadrature du Net* hanno raggiunto le medesime conclusioni rispetto alla conservazione di diverse categorie di dati. Innanzitutto è stato stabilito che, in ragione della idoneità degli indirizzi IP ad identificare una persona fisica proprietaria di un'apparecchiatura da cui viene effettuata una comunicazione via Internet[102] – e, pertanto, a rappresentare uno strumento vitale per lottare contro forme gravi di criminalità e prevenire minacce gravi alla sicurezza pubblica e nazionale – la loro raccolta generalizzata e indifferenziata risulta essere legittima in base al diritto UE, sempre che essa venga realizzata rispettando le "condizioni sostanziali e procedurali" atte a regolamentare l'uso dei dati in discussione[103]; condizioni, queste, che purtroppo non sono state specificate in alcun modo dalla Corte. Detta forma di conservazione è stata ugualmente dichiarata ammissibile con riferimento ai dati relativi all'identità civile, che contengono informazioni personali minime degli utenti dei mezzi di comunicazione elettronica, quali i loro indirizzi e coordinate[104]. A ciò si aggiunga che i giudici di Lussemburgo si sono occupati anche di un importante profilo procedurale, quello, cioè, dell'ammissibilità degli elementi di prova ottenuti tramite la conservazione indiscriminata dei dati ritenuta incompatibile con il diritto dell'Unione. A tal proposito, è stato sancito che, in forza del principio di effettività, la Direttiva n. 2002/58, interpretata alla luce della Carta di Nizza, impone al giudice penale nazionale di non tenere in considerazione le informazioni e gli elementi di prova ottenuti mediante codesto tipo di conservazione, nel contesto di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati, laddove siffatte persone "non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova"[105]. Attraverso questa formulazione, la Corte non ha fatto altro che stabilire implicitamente il principio secondo cui le prove ricavate da un'attività di raccolta indiscriminata delle informazioni personali contraria alla Direttiva n. 2002/58 ed agli articoli 7 e 8 della Carta UE sono valutabili da parte di un'autorità giudiziaria nazionale – e, dunque, ammissibili in un procedimento penale – qualora la persona interessata dalla sorveglianza sia posta nelle condizioni di confutare la legittimità delle prove medesime.

Le sentenze adottate dalla Corte di giustizia nei casi *Privacy International* e *La Quadrature du Net* assumono una certa rilevanza in quanto costituiscono uno spartiacque tra l'approccio particolarmente garantista espresso in passato e l'orientamento attuale, maggiormente sensibile al soddisfacimento delle esigenze securitarie: se è vero, difatti, che dette pronunce sembrano inizialmente consolidare la precedente prassi giurisprudenziale attenta al rafforzamento delle salvaguardie dei diritti contemplati dagli

[102] Ivi, par. 152.
[103] Ivi, parr. 155-156.
[104] Ivi, parr. 157-158.
[105] Ivi, par. 228; sul punto vedi anche: Court of Justice of the European Union, Press Release n. 123/20, *The Court of Justice Confirms that EU Law Precludes National Legislation Requiring a Provider of Electronic Communications Services to Carry Out the General and Indiscriminate Transmission or Retention of Traffic Data and Location Data for the Purpose of Combating Crime in General or of Safeguarding National Security*, 6 ottobre 2020, disponibile su curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf, pp. 3-4.

articoli 7 e 8 della Carta di Nizza – nella misura in cui confermano il divieto della conservazione generalizzata ed indifferenziata dei dati quale regola generale – è parimenti vero che le stesse si pongono in controtendenza rispetto a detta prassi, laddove statuiscono di converso numerose eccezioni alla regola citata, ammettendo in definitiva la conservazione indiscriminata e duratura di una vasta congerie di dati personali in numerose situazioni di specie[106].

In effetti, l'affermazione della legittimità ai sensi del diritto UE della conservazione diffusa e generalizzata di una serie indefinita ed estesa di dati delle comunicazioni – dati di traffico, quelli relativi all'ubicazione, gli indirizzi IP e i dati relativi alla identità civile –, prescindendo dall'esistenza di una connessione tra gli individui cui si riferiscono siffatti dati e gli obiettivi della sicurezza nazionale e pubblica perseguiti da tale raccolta, dà adito a forti dubbi e mal si concilia con i principi europei di proporzionalità, finalità limitata e di necessità, capisaldi alla base degli articoli 7 ed 8 della Carta UE[107].

Ciò è tanto più vero se si considera che questa affermazione non appare corredata da adeguate garanzie. In primo luogo, la mancata identificazione dei parametri atti a distinguere due nozioni facilmente sovrapponibili – quelle di sicurezza nazionale e di sicurezza pubblica[108] – è tale da permettere agli Stati di giustificare una conservazione massiva per conseguire obiettivi anche di sicurezza pubblica. In secondo luogo, la mancata individuazione e specificazione delle "condizioni sostanziali e procedurali", la cui osservanza legittimerebbe la raccolta indifferenziata degli indirizzi IP e dei dati relativi all'identità civile, non contribuisce alla certezza del diritto ed è idonea ad alimentare abusi del potere governativo. In terza analisi, in dispregio alle garanzie che devono informare il trattamento degli imputati nei procedimenti penali, è stata dichiarata l'ammissibilità dell'acquisizione e della valutazione in detti procedimenti di elementi di prova ottenuti mediante una conservazione indiscriminata e generalizzata contraria al

[106] In questo senso, vedi: X. TRACOL, *The Two Judgments of the European Court of Justice in the Four Cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber Is Trying Hard to Square the Circle of Data Retention*, in *Computer Law & Security Review*, 2021, vol. 41, pp. 1-13, disponibile su doi.org/10.1016/j.clsr.2021.105540, p. 10; M. ZALNIERIUTE, *The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments*, in *ASIL Insights*, 2020, n. 24, pp. 1-6, disponibile su www.asil.org/sites/default/files/ASIL_Insights_2020_V24_I28.pdf, p. 3; ID., *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union*, in *The Modern Law Review*, 2022, n. 1, pp. 198-218, pp. 217-218; M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in *European Public Law*, 2022, n. 28, pp. 123-154, disponibile anche su papers.ssrn.com/sol3/papers.cfm?abstract_id=3970756, pp. 1-24.

[107] J. SAJFERT, *Bulk Data Interception/Retention Judgments of the CJEU. A Victory and a Defeat for Privacy*, 26 ottobre 2020, disponibile su europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/.

[108] In relazione a questo aspetto, vedi: L. VARDANYAN, V. STEHLÍK, *Schrems II: Will It Really Increase the Level of Privacy Protection Against Mass Surveillance?*, in *Bratislava Law Review*, 2020, n. 4, pp. 111-128, p. 123; PRIVACY LAW BARRISTER, *Mass Surveillance of Electronic Communications: Recent Developments*, 26 ottobre 2020, disponibile su privacylawbarrister.com/2020/10/26/mass-surveillance-of-electronic-communications-recent-developments/.

diritto UE, nella misura in cui la persona riguardata da codesta conservazione possa contestare la legittimità di siffatti elementi.

Questo orientamento espresso nel caso *La Quadrature du Net* è stato altresì confermato dalla Corte di giustizia in due recenti sentenze inerenti a questioni pregiudiziali relative anch'esse all'interpretazione dell'articolo 15 della Direttiva 2002/58: la prima resa nel marzo 2021 nel caso *H.K. c. Prokuratuur*; la seconda, recentemente adottata nell'aprile 2022 nel caso *G.D. c. Commissioner of An Garda Síochána*. Dette sentenze hanno riguardato il profilo della compatibilità di talune normative nazionali attinenti alle comunicazioni elettroniche – rispettivamente quella estone e quella irlandese – con i pertinenti parametri contemplati dal diritto UE in materia di tutela della vita privata e dei dati personali[109]. Ebbene, in entrambe le pronunce i giudici di Lussemburgo hanno ribadito l'abbandono all'approccio garantista definito nelle decisioni *Tele2 Sverige*, *Ministerio Fiscal Schrems I e II*, rafforzando la validità delle argomentazioni elaborate nei casi *Privacy International* e *La Quadrature du Net*, in special modo quelle concernenti tanto la legittimità della conservazione generalizzata ed indifferenziata dei dati di traffico, dei dati relativi all'ubicazione, degli indirizzi IP e dei dati relativi all'identità civile[110], quanto l'ammissibilità delle prove ottenute attraverso una raccolta di dati contraria alla rilevante normativa europea sulla privacy[111].

5. Conclusioni e prospettive

Nel corso del presente contributo è stato dimostrato che la Corte europea dei diritti dell'uomo e la Corte di giustizia dell'Unione europea hanno espresso nel corso degli anni posizioni coincidenti: esse, infatti, in una prima fase hanno escluso categoricamente la legittimità della conservazione indifferenziata ed indiscriminata dei dati personali in base rispettivamente alla CEDU ed al pertinente diritto UE; in una seconda fase hanno manifestato, invece, una posizione differente, dichiarando l'ammissibilità della conservazione in esame, sempre che in generale vengano rispettate alcune (non propriamente ed adeguatamente definite) condizioni sostanziali e procedurali[112]. Si è

[109] Per un'analisi di tali decisioni, vedi: G. NADDEO, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in questa *Rivista*, 2022, n. 2, pp. 188-217.

[110] Corte di giustizia, Grande Sezione: sentenza del 2 marzo 2021, *H.K. c. Prokuratuur*, causa C-746/18, parr. 30-38; sentenza del 5 aprile 2022, *G.D. c. Commissioner of An Garda Síochána e altri*, causa C-140/20, parr. 57-67.

[111] Corte di giustizia, Grande Sezione, *Prokuratuu*r, cit., parr. 41-44; *Commissioner of An Garda Síochána* cit., parr. 117, 128.

[112] In questo senso, vedi anche le condivisibili considerazioni di alcuni autori, secondo cui, con riferimento alla sorveglianza di massa dei dati personali: "a more careful reading of Quadrature du Net and Big Brother Watch reveals that the CJEU and the ECtHR are not really walking in different directions. This is evidenced by several reasons. Both Courts have opted for a more nuanced approach to bulk surveillance, which is prescribed by several procedural guarantees regarding authorisation, retention, access and oversight. Such guarantees, conditions and safeguards demonstrate a trend towards a 're-modulation' of the prohibition of bulk surveillance, with the adoption of a more proceduralised approach. Moreover, the CJEU laid down in

assistito dunque ad un graduale cambio di paradigma tra sicurezza e privacy, che conduce alla normalizzazione della conservazione massiva dei dati personali per finalità di contrasto al terrorismo ed a forme gravi di criminalità. In definitiva, le autorità giurisdizionali europee nell'attività di bilanciamento tra privacy e sicurezza sembrano allo stato propendere maggiormente verso la valorizzazione ed il rafforzamento delle esigenze securitarie, consentendo alle autorità statali l'adozione di misure invasive della vita privata dei soggetti interessati alla sorveglianza e rendendo quindi concretamente realizzabili gli abusi del potere esecutivo.

Quanto al contesto del Consiglio d'Europa, va detto che alla luce del fatto che la CEDU è stata storicamente considerata alla stregua di uno "strumento vivente" da interpretarsi "in the light of present-day conditions"[113], potrebbe ritenersi che l'approccio dei giudici di Strasburgo sia teso a rielaborare il contenuto dell'articolo 8, prospettando una nuova concezione del diritto alla vita privata tramite la riduzione delle garanzie ad esso sottese[114]. Tuttavia, è possibile contrapporre a questo approccio l'imprescindibile rilievo rappresentato dal fatto che la Convenzione europea dei diritti dell'uomo risulta essere uno strumento giuridico di vitale importanza, predisposto dopo la Seconda Guerra mondiale, con l'obiettivo primario di salvaguardare i diritti umani a fronte della invasività dei poteri statali e non, viceversa, di assecondare l'ampliamento di tali poteri.

Quanto al contesto UE, va osservato che la Corte di Lussemburgo ha tentato, pur senza riuscirci adeguatamente, di giustificare in base al diritto UE misure idonee a pregiudicare la vita privata di una moltitudine di persone, cercando di ricondurre faticosamente le medesime misure nell'alveo protettivo degli articoli 7 ed 8 della Carta UE. Ciò, tanto mediante la previsione di eccezioni al divieto della conservazione generalizzata e diffusa dei dati personali, quanto attraverso l'affermazione di garanzie sostanziali e procedurali di difficile declinazione ed individuazione.

Pertanto, le corti europee nella seconda fase della loro giurisprudenza non hanno affrontato in maniera appropriata il nodo gordiano concernente il paradigma in questione, non rispondendo in maniera dettagliata e precisa al seguente, fondamentale quesito, ovvero: come ed a quali condizioni è possibile giustificare la conservazione massiva ed indiscriminata delle informazioni personali alla luce dei principi internazionali ed europei di finalità limitata, proporzionalità, necessità e minimizzazione dei dati, che costituiscono i capisaldi alla base delle tutele *ex* articoli 8 della CEDU, e 7 e 8 della Carta UE?

È auspicabile dunque che nell'immediato futuro siffatte corti tornino alle origini, riavvicinandosi agli orientamenti espressi nella prima fase della loro prassi – nelle

Quadrature du Net various permissible types of bulk surveillance with significant repercussions" (M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net,* cit., pp. 18-19, 23-24).

[113] Come è noto, l'approccio ermeneutico teso a configurare la Convenzione europea dei diritti umani quale strumento vivente, elaborato dalla Corte europea per la prima volta nel caso *Tyrer* (Corte europea dei diritti dell'uomo, Camera, sentenza del 25 aprile 1978, ricorso n. 5856/72, *Tyrer c. Regno Unito*) e da essa costantemente ribadito nel corso degli anni, costituisce un metodo di estrema rilevanza nel sistema complessivo della CEDU.

[114] J.-P. FOEGLE, *La Cour européenne des droits de l'homme procède à une condamnation en demi-teinte de la surveillance "de masse"*, in *La Revue des droits de l'homme* [en ligne], 26 ottobre 2018, disponibile su journals.openedition.org/revdh/4865, pp. 1-5, p. 4.

decisioni *Zakharov* e *Szabó e Vissy* (CEDU) e nelle pronunce *Tele2 Sverige*, *Ministerio Fiscal*, *Schrems I* e *II* (CGUE) – dichiaratamente contrari alla raccolta indifferenziata e diffusa dei dati e volti alla effettiva salvaguardia dei diritti alla vita privata ed alla protezione dei dati.

È auspicabile, inoltre, che detta inversione di rotta possa avvenire il prima possibile, in ragione della circostanza che nel 2019 il Consiglio UE ha portato a termine il processo di riflessione sulla *data retention* per finalità di contrasto alla criminalità invitando la Commissione a rielaborare la normativa sulla conservazione delle informazioni personali[115] [segnatamente: la Direttiva n. 2002/58[116]; il Regolamento europeo sulla protezione dei dati; e la Direttiva sulle attività di contrasto (cd. Direttiva polizia)[117]]. Ciò nella prospettiva vuoi di dotare le autorità statali di maggiori poteri ai fini dell'acquisizione di un'ampia congerie di dati nella lotta al terrorismo ed alle forme gravi di criminalità, vuoi di conseguire una maggiore uniformità legislativa tra i vari Stati membri in questo determinato settore[118]. Tra l'altro, la necessità di un cambio di rotta in tal senso si rende sempre più urgente se si considera che il Consiglio UE ha manifestato l'esigenza che siffatto processo di rielaborazione tenga in debito conto i principi espressi nei casi *Privacy International*, *La Quadrature du Net* e *H.K. c. Prokuratuur*[119].

Laddove le corti europee, baluardi insostituibili della tutela dei diritti umani in Europa, confermino l'atteggiamento mostrato nella seconda fase del loro percorso giurisprudenziale, la possibilità che per i prossimi decenni venga legittimata e normalizzata una sorveglianza massiva dei dati personali lesiva degli articoli 7 e 8 della Carta UE e 8 della CEDU è molto concreta, con conseguenti rischi di gravi pregiudizi e restrizioni ingiustificate del diritto alla vita privata e dei dati personali di una moltitudine di persone. Porre un argine alla invasività dei pubblici poteri e delle autorità di

[115] M. ZALNIERIUTE, *The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments*, in *ASIL Insights*, 2020, n. 24, disponibile su www.asil.org/sites/default/files/ASIL_Insights_2020_V24_I28.pdf, pp. 4-5; Conclusioni del Consiglio dell'Unione europea sulla conservazione dei dati per finalità di lotta contro la criminalità, del 27 maggio 2019, Doc. 9663/19, disponibile su data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/it/pdf.

[116] Nel 2017 è stata già presentata una proposta per adottare un nuovo regolamento sulla vita privata e le comunicazioni elettroniche (cd. Regolamento sull'e-privacy) con l'obiettivo di sostituire la Direttiva n. 2002/58 (vedi: Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (vedi: COM/2017/010 final - 2017/03, disponibile su eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52017PC0010).

[117] 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 del 4 maggio 2016, pp. 1-88; Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in GUUE L 119 del 4 maggio 2016, pp. 89-131.

[118] Conclusioni del Consiglio dell'Unione europea sulla conservazione dei dati per finalità di lotta contro la criminalità, del 27 maggio 2019, Doc. 9663/19, cit., parr. 3-5, pp. 2-3.

[119] Ivi, par. 8, p. 4; sul punto, vedi: M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, cit., pp. 117-118.

intelligence risulta, quindi, di primaria importanza allo scopo di evitare che un nuovo modello statale basato sulla società del controllo – preconizzato da George Orwell nel suo romanzo "1984", anche attraverso la nota formula "Big Brother is watching you" – possa pericolosamente materializzarsi nella vita reale dei cittadini europei.

ABSTRACT: Il presente lavoro ha ad oggetto l'analisi della legittimità della sorveglianza massiva dei dati personali in base al diritto internazionale ed europeo alla luce della prassi giurisprudenziale adottata dalla Corte europea dei diritti dell'uomo e dalla Corte di giustizia dell'Unione europea. Nel contributo viene esaminato un importante cambio di approccio espresso nel corso degli anni da dette corti: da un lato, nella prima fase della loro prassi è stata sancita l'incompatibilità della raccolta indiscriminata e diffusa delle informazioni personali con la Convenzione europea dei diritti dell'uomo e la pertinente normativa UE in materia di privacy individuale; dall'altro, nella seconda fase è stata affermata peraltro la legittimità di detta raccolta. Nel contributo viene sottolineato che tale nuovo orientamento, basato sul cambio di paradigma tra privacy e sicurezza e teso a normalizzare la sorveglianza di massa nella lotta al terrorismo ed alla criminalità organizzata, pone una serie di delicate problematiche con riguardo all'osservanza dei diritti umani tutelati tanto dal sistema di Strasburgo quanto dal diritto dell'Unione europea.

KEYWORDS: sorveglianza massiva dei dati personali – Corte europea dei diritti dell'uomo – Corte di giustizia dell'Unione europea – diritto alla protezione dei dati personali e della vita privata – tutela degli interessi statali.

THE NORMALIZATION OF MASS SURVEILLANCE IN THE CASE-LAW OF STRASBOURG AND LUXEMBOURG COURTS: TOWARDS A PARADIGM SHIFT IN THE PRIVACY VS. SECURITY RELATIONSHIP

ABSTRACT: This essay deals with the analysis of the legality of the mass surveillance of personal data under international and European law in the light of the case law of the European Court of Human Rights and the Court of Justice of the European Union. The contribution examines an important change of approach expressed over the years by these courts: on the one hand, in the first phase of their case law, the Courts had established the incompatibility of the indiscriminate and widespread collection of personal information with the European Convention on Human Rights and the relevant EU legislation on individual privacy; on the other hand, in the second phase the legality of said collection was affirmed. The article underlines that this new orientation, based on the paradigm shift between privacy and security and aimed at normalizing mass surveillance in the fight against terrorism and organized crime,

raises several and complex issues with regard to the observance of human rights protected both by the Strasbourg system and by European Union law.

KEYWORDS: mass surveillance of personal data – European Court of Human Rights – Court of Justice of the European Union – right to the protection of personal data and privacy – protection of State interests.