AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Le intercettazioni di massa all'esame della CEDU

di Paolo Viafora

23 febbraio 2023

Sommario: 1. Premessa. – 2. I tratti distintivi delle intercettazioni di massa. – 3. La genesi dei casi e i conseguenti criteri ex art. 8 identificati dalla Corte. – 4. L'esame dei casi *sub iudice*. – 4.1 Accessibilità. – 4.2 I casi in cui le intercettazioni possono essere autorizzate. – 4.3 Le circostanze in cui le comunicazioni di un individuo possono essere intercettate. – 4.4 La procedura di autorizzazione. – 4.5 La procedura di selezione, esame ed uso del materiale intercettato. – 4.6 La condivisione del materiale con terze parti. – 4.7 I limiti di durata delle intercettazioni, di conservazione del materiale e le circostanze in cui questo può essere cancellato o distrutto. – 4.8 La supervisione delle operazioni. – 4.9 Il controllo post-fatto. – 4.10 I relativi metadati. – 4.11 Le conclusioni della Corte. – 5. Il diritto alla libertà di espressione. – 6. La ricezione di informazioni da servizi d'intelligence estera. – 7. Considerazioni a margine delle sentenze. – 8. Conclusioni.

1. Premessa

Spinti dalla necessità di affrontare nuove minacce sempre più eterogenee e far fronte ad una platea quanto mai variopinta di attori internazionali che usano l'etere per veicolare attacchi e moltiplicare la propria forza, gli Stati moderni registrano un crescente ricorso, in chiave soprattutto preventiva, all'uso delle intercettazioni di massa per finalità di pubblica sicurezza e protezione dello Stato democratico. Tali strumenti, però, proprio in virtù di quelle caratteristiche di pervasività che li rendono così efficaci mezzi d'*intelligence* e li distinguono dalle intercettazioni "tradizionali", pongono evidenti problemi di bilanciamento con vari diritti essenziali alla sussistenza dello stesso Stato democratico, primi tra tutti il diritto alla riservatezza e alla libertà d'espressione; la cui fruizione è necessario presupposto di tutta una serie di diritti e libertà – si pensi al diritto di voto o di sciopero – che solo al riparo dallo sguardo indiscreto dei detentori del potere pubblico possono liberamente esercitarsi. Evidente, dunque, la problematicità della materia, giacché in essa emerge palese l'antinomia esistente laddove la tutela dell'ordine democratico passi attraverso la compressione di alcune sue garanzie distintive; così come evidente è la necessità per gli operatori del diritto di trovare soluzioni a tale antinomia che permettano agli apparati pubblici di

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

adeguarsi allo "spirito del tempo" senza che ciò significhi, come spesso è accaduto, immolare alla sicurezza la libertà dei consociati.

Tale fenomeno e le sue problematiche costituiscono l'oggetto delle recenti sentenze rese dalla Gran Camera della Corte Europea dei Diritti dell'Uomo[1] nei casi *Big Brother Watch c. Regno Unito*[2] e *Centrum för Rättvisa c. Svezia*[3] che, pur con i limiti e le perplessità che si esporranno, rappresentano il più recente approccio alla materia delle intercettazioni di massa di uno tra i principali meccanismi internazionali di tutela dei diritti dell'uomo e, innovando la stessa giurisprudenza CEDU fissata nei casi *Liberty e altri c. Regno Unito* e *Weber e Saravia c. Germania*,[4] marcano una tappa storica nell'esame critico del fenomeno e nel tentativo di adeguarne le asperità al rispetto dei diritti umani previsti dalla Convenzione. Del resto, è la stessa Corte EDU a dare atto della necessità di adeguare la propria giurisprudenza ai tempi, riconoscendo che pur avendo già esaminato le intercettazioni di massa nei casi ora citati, «questi hanno adesso più di dieci anni, anni in cui lo sviluppo tecnologico ha significativamente cambiato il modo in cui le persone comunicano. Le vite vengono sempre più vissute online, generando sia un volume di comunicazioni significativamente maggiore che comunicazioni di natura e qualità significativamente differente, rispetto a quelle che potevano essere generate dieci anni fa. Per cui minore era la portata delle attività di sorveglianza considerate in quei casi».[5]

Scopo del presente contributo è dunque quello di ricostruire l'approccio della Corte al tema delle intercettazioni di massa attraverso l'esame delle recenti decisioni in cui questo si è estrinsecato, identificando i principi *ivi* fissati a disciplina della materia, le questioni tuttora rimaste aperte e da ciò traendo considerazioni di ordine più generale sui peculiari caratteri che le minacce allo Stato assumono nel mondo contemporaneo e

[1] D'ora in poi abbreviata anche in "CEDU", la "Corte", "Corte di Strasburgo" o "Corte EDU".
[2] Corte Europea dei Diritti dell'Uomo, Gran Camera, 25 maggio 2021, cause 58170/13, 62322/14 e 24960/15, *Case of Big Brother Watch and Others v. The United Kingdom*. Di seguito, brevemente, *Big Brother Watch.*
[3] Corte Europea dei Diritti dell'Uomo, Gran Camera, 25 maggio 2021, causa 35252/08, *Case of Centrum för Rättvisa v. Sweden*. Di seguito, brevemente, *Centrum för Rättvisa.*
[4] Rispettivamente, Corte Europea dei Diritti dell'Uomo, Quarta sezione, 1° luglio 2008, causa 58243/00, *Case of Liberty and Others v. The United Kingdom* e Corte Europea dei Diritti dell'Uomo, Terza sezione, causa 54934/00, *Decision as to the admissibility of Application no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany*. Si noti che a differenza di tali decisioni, frutto della Terza e Quarta sezione della Corte, i casi odierni costituiscono elaborazione della Grande Camera.
[5] Testualmente, « *However, while the bulk interception regimes considered in those cases were on their face similar to that in issue in the present case, both cases are now more than ten years old, and in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago. The scope of the surveillance activity considered in those cases would therefore have been much narrower*». Cfr. caso *Big Brother Watch*, n. 2 cit., §341 (Traduzione italiana del presente autore).
A proposito della differente portata delle moderne intercettazioni di massa, è interessante notare che il caso *Liberty* riguardava l'attività di impianti capaci di intercettare "soli" 10.000 canali telefonici. Cfr. caso *Liberty*, n. 4 cit., §5.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

le loro implicazioni sul fronte dei diritti umani. Ovviamente, tali decisioni potranno leggersi correttamente solo alla luce degli specifici caratteri del mezzo in esame. Questo rappresenta perciò il naturale punto di partenza dell'analisi.

2. I tratti distintivi delle intercettazioni di massa

Nella visione datane dalla CEDU stessa, le intercettazioni di massa rappresentano un processo graduale che vede l'interferenza con il diritto alla vita privata degli intercettati aumentare col progredire di fasi che, generalmente, possono così riassumersi: (a) captazione e conservazione iniziale di dati e metadati[6] (anche noti come comunicazioni e dati di comunicazione, nel linguaggio della Corte), (b) applicazione ad essi dei selettori, (c) esame dei dati/metadati da ciò risultati più rilevanti e (d) successivo uso del prodotto finale nonché eventuale trasmissione a terze parti.[7] L'art. 8 entra in gioco in ciascuna di queste fasi, anche se l'interferenza è tanto più marcata quanto più avanzata è la fase.[8] A differenza delle tradizionali misure di sorveglianza segreta finora ad oggetto della giurisprudenza della Corte, le intercettazioni di massa presentano, però, vari tratti innovativi; anzitutto rispetto alle intercettazioni mirate.

Invero, come le rispettive denominazioni rendono palese, le intercettazioni mirate pongono a proprio bersaglio uno o più individui determinati ed in virtù di ciò vengono normalmente compiute mettendo sotto controllo direttamente gli apparecchi a questi in uso, giacché e lì che è lecito presumere confluiranno le conversazioni loro destinate.[9] Per contro, le intercettazioni di massa non si rivolgono di principio ad un bersaglio specifico ma mirano a monitorare indistintamente tutto il traffico di dati e metadati in transito per un determinato punto di raccolta. È il successivo uso di selettori – ossia di filtri quali, ad esempio, parole chiave o indirizzi e-mail – che raffina la massa aggregata di dati inizialmente captati permettendo di individuarvi le conversazioni di maggior interesse quanto a contenuto o soggetti coinvolti.[10] Ciò, a sua volta, trova spiegazione nelle differenti finalità perseguite, visto che mentre le intercettazioni mirate sono generalmente impiegate nelle indagini criminali, dove si ha una platea perlopiù definita di soggetti sospettati, le intercettazioni di massa sono usate prevalentemente per l'identificazione a fini di *intelligence* di minacce provenienti da una compagine indefinita di attori, i cui segni distintivi vanno ricercati all'interno di una gran massa

[6] Concernenti, cioè, non già il contenuto della comunicazione, ma le sue coordinate fondamentali quali data e ora, posizione e identità delle parti. Così I. SIGISMONDI, *Telematica* [dir. cost.], in Enc. Online Trec., §7. Ultimo accesso effettuato il 30.09.2022 presso «https://www.treccani.it/enciclopedia/telematica-dir-cost_%28Diritto-on-line%29/».
[7] *Big Brother Watch*, n. 2 cit., §325.
[8] Ibid. 330.
[9] È quanto si desume *a contrario*, per esempio, dal ragionamento della Corte in *Big Brother Watch*, n. 2 cit., §346.
[10] Cfr. *Big Brother Watch*, n. 2 cit., §17.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

eterogenea di informazioni.[11] Non ultimo, la natura transnazionale di molte minacce fa sì che spesso le intercettazioni di massa si rivolgano alle comunicazioni internazionali (vale a dire transfrontaliere) di soggetti al di fuori della giurisdizione territoriale dello Stato, per i quali procedere ad altre forme di sorveglianza risulterebbe impraticabile: mentre è infatti di tutta evidenza che gli individui, così come gli strumenti che questi usano per relazionarsi con il mondo, essendo dotati di corporalità, si trovano concretamente nel dominio riservato di uno Stato che dovrebbe necessariamente violarsi, le risultanti comunicazioni hanno invece forma immateriale e transitano lungo le reti globali senza alcun significativo riferimento ai confini nazionali, perciò non dando luogo ai problemi prima esposti.[12]

A ciò si affiancano considerazioni di ordine più generale: il crescente tempo speso dalla popolazione su internet rende accessibile all'autorità una porzione esponenzialmente maggiore delle loro vite private e anche quando il contenuto di tali comunicazioni risulta privo di pregio, i relativi dati di comunicazione forniscono una rilevante quantità di informazioni personali sugli interlocutori, quali posizione e identità; intrusione peraltro amplificata dalla loro acquisizione in massa.[13] Allo stesso modo, il legittimo bisogno di segretezza sotteso alle intercettazioni di massa implica inevitabilmente che per ragioni di sicurezza le autorità nazionali, nel condurle, useranno il massimo riserbo, così aprendole all'inerente rischio di abusi.[14] Risulta perciò evidente come le intercettazioni di massa costituiscano interferenze di quantità e qualità significativamente superiore rispetto alle tradizionali misure di sorveglianza.

3. La genesi dei casi e i conseguenti criteri ex art. 8 identificati dalla Corte

La genesi dei casi *Big Brother Watch* e *Centrum för Rättvisa* deve ricercarsi esattamente nell'acceso dibattito pubblico sorto in merito all'uso delle intercettazioni di massa da parte degli Stati, in virtù della particolare invasività di tale strumento e del suo conseguente impatto sui diritti e libertà democratici.

In particolare, nel Regno Unito, a seguito delle rivelazioni di Edward Snowden sulle intercettazioni di massa condotte dai servizi segreti nazionali,[15] diverse organizzazioni per i diritti civili ritenevano di poter esserne state vittime per via della sensibilità delle proprie comunicazioni (inerenti associazioni non governative, informatori, avvocati e vittime di abusi) nonché dei mezzi con cui queste erano state

[11] Ibid.
[12] Cfr. Ibid. §322. *Centrum för Rättvisa*, n. 3 cit., §258.
[13] *Big Brother Watch*, n. 2 cit., §341-342.
[14] Ibid. §349.
[15] Si veda: G. GREENWALDG, *Revealed: how US and UK spy agencies defeat internet privacy and security*, in *The Guardian* (6 giugno 2013), consultabile presso «https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order». Ultimo accesso eseguito il 21.11. 2022. Vedasi anche F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*, 26 giugno 2013.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

compiute (chiamate, videochiamate, email, chat, ...); veniva inoltre contestata la prassi britannica di scambio delle intercettazioni con i servizi segreti statunitensi.[16] In tale clima, un non irrilevante numero di tali organizzazioni ricorreva direttamente[17] o a seguito del previo esaurimento dei rimedi domestici alla CEDU,[18] lamentando un'incompatibilità del regime di intercettazioni di massa britannico con i loro diritti alla vita privata (art. 8 della Convezione) e alla libertà di espressione (art. 10). Similmente, in Svezia, la questione della compatibilità alla CEDU del locale regime di sorveglianza di massa veniva sollevata da un'associazione non governativa e faceva seguito all'acceso interesse mostrato dal governo verso tale tecnica di sorveglianza attraverso l'adozione di una corposa legislazione sul punto, ma mirava allo scopo leggermente diverso di migliorare tali norme e non bandire del tutto la sorveglianza di massa.[19]

Recependo in parte tali istanze della società civile, le decisioni della Corte tentano di aggiornare i canoni definiti per le misure di sorveglianza classiche adattandoli ai tratti innovativi delle intercettazioni di massa, ma ciò fanno nell'ambito dei tradizionali principi legittimanti l'invasione della sfera privata dei cittadini, dettati dalla Corte nella sua risalente giurisprudenza.

Da un lato, ed a dispetto dei ravvisati mutamenti sociali e tecnologici, viene così ribadita la perdurante vitalità della giurisprudenza CEDU relativa all'art. 8, secondo cui le interferenze col diritto alla vita privata possono dirsi giustificate quando α) perseguono uno scopo legittimo, β) appaiono necessarie in una società democratica per raggiungere tale scopo e γ) sono conformi alla legge.[20] Ciò richiedendo a sua volta che le disposizioni che le disciplinano siano accessibili e prevedibili, ed intendendosi per prevedibilità nel contesto della pubblica sorveglianza non che il cittadino debba sapere quando le autorità ricorreranno a tali misure – cosa che ovviamente renderebbe le

[16] 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 (EDPL)*, vol. 5, no. 2, 2019, 253-254.

[17] Tale 'aggiramento' – per così dire – dell'ordinaria via di accesso alla CEDU costituita dal previo esaurimento dei rimedi domestici faceva seguito alla conclusione raggiunta dalla Corte stessa nel caso *Kennedy v The United Kingdom*, nel quale, l'*Investigatory Powers Tribunal* (IPT), vale a dire l'autorità innanzi la quale i ricorrenti avrebbero dovuto presentare reclamo nel Regno Unito, era stato giudicato un rimedio non effettivo. È interessante notare che la CEDU, pur riconoscendo che successivamente al caso *Kennedy* l'IPT avesse dato prova di efficacia, condona la scorciatoia presa dai ricorrenti dicendo che questi non si possono biasimare per aver dato fede ad una pronuncia CEDU. Sennonché, come giustamente notato dalla dottrina, tale atteggiamento ha l'inconveniente di trasformare il criterio del previo esaurimento dei rimedi domestici da oggettivo in soggettivo, visto che a contare è, in ultima analisi, non l'effettività del rimedio ma cosa i ricorrenti credono quanto ad essa. Cfr. Ibid. § 2.

[18] In tali casi, sul piano domestico, l'IPT concludeva che prima che le autorità competenti rendessero innanzi ad esso i dovuti chiarimenti, il regime britannico di intercettazioni di massa risultasse in contrasto con gli artt. 8 e 10 Conv. EDU, ma tale lacuna dovesse ritenersi sanata proprio dall'avvenuta divulgazione. Ciò portava i ricorrenti ad adire la Corte di Strasburgo. Ibid. 254.

[19] M. KLAMBERG, *Big Brother's Little, More Dangerous Brother: Centrum för Rättvisa v. Sweden*, in *VerfassungsBlog*, 01 giugno 2021. Consultabile presso «https://verfassungsblog.de/raettvisa/» Ultimo accesso eseguito il 21.11. 2022.

[20] *Big Brother Watch*, n. 2 cit., §332.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

intercettazioni vane – bensì che la legge nazionale identifichi con sufficiente chiarezza le circostanze e condizioni che titolano le autorità a ricorrervi.[21]

Dall'altro, si postula la necessità di superare le "cautele minime" precedentemente richieste alle legislazioni nazionali in materia di intercettazioni mirate e consistenti nella definizione:

1) Della natura dell'offesa che può dare luogo ad un ordine di intercettazione
2) Delle categorie di persone le cui conversazioni appaiono suscettibili di venir intercettate
3) Del limite di durata delle intercettazioni
4) Della procedura da seguire per esaminare, usare e conservare i dati ottenuti
5) Delle precauzioni da assumere nella comunicazione dei dati a terze parti e
6) Delle circostanze in cui dati intercettati possono o devono essere eliminati.

in quanto ritenute inidonee a disciplinare i peculiari tratti, strutturali e teleologici, che caratterizzano il nuovo mezzo in esame.[22] Ne consegue che i primi due dei sei parametri sopra riportati – la natura dell'offesa e le categorie di persone coinvolte – vengono ritenuti non immediatamente applicabili al nuovo strumento giacché, pur indefettibilmente presenti nel contesto delle indagini criminali cui si rivolgono le intercettazioni mirate, mal si concilierebbero con la 'lotta all'ignoto' condotta a mezzo delle intercettazioni di massa. Del pari, il requisito del ragionevole sospetto invocato da varie parti quale presupposto delle captazioni,[23] viene invece ritenuto dalla Corte inapplicabile nel contesto della sorveglianza di massa sulla scorta della finalità in principio preventiva di quest'ultima, come tale priva di specifici bersagli e/o crimini definiti.[24]

Punto di partenza nella definizione del nuovo regime diventa dunque la considerazione della diversa finalità del mezzo e dell'intrinseco bisogno di segretezza ad esso sotteso, che esponendo le intercettazioni di massa ad evidenti rischi di abusi da parte degli Stati rende necessario attorniarle di "garanzie da capo a capo",[25] identificate dalla Corte nella necessità a livello domestico di:

1) Verificare ad ogni passaggio la necessità e proporzionalità delle misure in corso d'adozione
2) Sottoporre ad autorizzazione indipendente l'inizio delle operazioni, nonché
3) Sottoporre lo svolgersi delle operazioni a supervisione e revisione *ex post facto* indipendente

[21] Ibid. §333.
[22] Ibid. §§335, 347. Trattasi di scelta quantomai rilevante soprattutto se si considera che con essa la Gran Camera abbraccia una tesi diametralmente opposta a quella fatta propria dalla Prima Sezione nel precedente grado di giudizio ritenendo errato assumere che le intercettazioni di massa costituissero intrusioni nella vita privata maggiori rispetto alle tradizionali misure di sorveglianza. Cfr. Corte Europea dei Diritti dell'Uomo, Prima Sezione, 13 settembre 2018, cause 58170/13, 62322/14 e 24960/15, *Case of Big Brother Watch and Others v. The United Kingdom*, §316.
[23] Cfr. *Big Brother Watch*, n. 2 cit, §§281, 316 e 318. *Centrum för Rättvisa*, n. 3 cit., § 186.
[24] *Big Brother Watch*, n. 2 cit., §348. *Centrum för Rättvisa*, n. 3 cit., § 262.
[25] Letteralmente "end-to-end safeguards", così *Big Brother Watch*, n. 2 cit., §350. Cfr. anche §349.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Per contro, deve osservarsi che l'autorizzazione giudiziaria – pur ritenuta in principio preferibile – non viene fatta dalla Corte oggetto di uno specifico requisito, ritenendosi sufficiente che tale compito sia assolto da un corpo indipendente dall'Esecutivo, ed analoghe considerazioni sono ripetute per la revisione *ex post*. Allo stesso modo, se è vero che per la fase di autorizzazione e revisione delle intercettazioni si prevedono diverse garanzie (rispettivamente, l'obbligo di portare a conoscenza l'autorità indipendente degli obiettivi delle intercettazioni e dei canali di comunicazione suscettibili di essere intercettati, nonché l'attribuzione all'autorità di revisione di poteri vincolanti di cessazione delle intercettazioni e distruzione del relativo materiale in caso di accertata violazione) è pur vero che in entrambi tali fasi le peculiarità delle intercettazioni di massa ispirano alcuni compromessi.[26]

È il caso dell'autorizzazione dei selettori. Qui, la Corte riconosce che l'uso di tali elementi costituisce un passaggio fondamentale delle intercettazioni, rappresentando il punto in cui queste possono iniziare a bersagliare uno o più soggetti e determinare quali conversazioni formeranno oggetto di esame degli analisti ma, tenendo conto dell'ampio numeri di selettori necessari nelle intercettazioni di massa e la connessa necessità di flessibilità degli Stati nella loro scelta – dunque accogliendo le loro obiezioni – rinuncia ad enunciare un obbligo di elencazione specifica, limitandosi a chiedere che l'autorizzazione contenga la generica indicazione dei tipi o delle categorie di selettori impiegati.[27] Solo per l'uso dei selettori forti (ossia relativi ad un individuo definito) vengono richieste cautele aggiuntive, prevedendosi che l'uso di ognuno di questi venga giustificato quanto a necessità e proporzionalità e sottoposto a previa autorizzazione interna.[28]

Analogamente, pur riconoscendo l'imprescindibilità di garantire alle persone rimedi idonei a mettere in discussione la compatibilità delle intercettazioni che li vedessero coinvolti, la Corte evita di sancire un vero e proprio obbligo di notifica nei loro confronti, notando che nel contesto delle intercettazioni di massa rimedi "non recettizi" possono offrire talvolta garanzie addirittura maggiori di quelli basati sulla notifica e ciò perché queste bersagliano principalmente soggetti al di fuori della giurisdizione dello Stato – di cui le autorità potrebbero perciò ignorare il domicilio – e visto in ogni caso che la notifica potrebbe essere privata di effetti pratici con l'invocazione di ragioni ostative di sicurezza nazionale.[29]

Alla luce di quanto sopra, appare evidente il compromesso ricercato dalla Corte tra salvaguardia dei diritti umani coinvolti nelle captazioni e volontà di non ingessare eccessivamente l'azione statale nella loro conduzione; opera che trova definitiva consacrazione ed enunciazione sistematica nella lista delle otto, nuove, garanzie minime, a mente delle quali le legislazioni nazionali devono ora definire:

[26] Ibid. §§349-350, 358.
[27] Ibid. §§353-354.
[28] Ibid. §355.
[29] Ibid. §358.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

1) I casi in cui le intercettazioni possono essere autorizzate
2) Le circostanze in cui le comunicazioni di un individuo possono essere intercettate
3) La procedura da seguire per il rilascio dell'autorizzazione
4) La procedura da seguire per la selezione, l'esame e l'uso del materiale intercettato
5) Le precauzioni da adottare nella trasmissione del materiale a terze parti
6) I limiti di durata delle intercettazioni, di conservazione del materiale e le circostanze in cui questo materiale può essere cancellato o distrutto
7) Le procedure e modalità con cui l'autorità indipendente monitora il rispetto dei parametri precedenti e i suoi poteri in caso di violazioni, nonché
8) Le procedure per la revisione *ex post facto* indipendente e i poteri conferiti a tale autorità per fronteggiare i casi di violazione[30]

Come si può notare, il nuovo test individuato dalla Corte costituisce una versione riveduta ed estesa dei sei criteri precedenti, in cui la necessaria indicazione dei tipi di reati legittimanti l'intercettazione e delle persone destinatarie della misura (cautele proprie di strumenti di sorveglianza per finalità di contrasto al crimine), lascia il posto al dovere di individuare *ex ante* casi e modi di ricorso alle intercettazioni (quali necessari corollari di un mezzo preventivo), ed a quello di definire appropriate procedure di autorizzazione, supervisione e riesame idonee ad evitare un utilizzo estensivo o abusivo del mezzo.

A ciò si aggiunge una serie ulteriore di criteri per la condivisione dei dati così ottenuti, frutto del ripensamento della Corte quanto all'opportunità di definire specifiche cautele in tal senso. Alla luce di questi, possono costituire oggetto di trasferimento solo le comunicazioni raccolte e conservate in conformità alla Convenzione (in conformità, dunque, agli otto punti sopra descritti) e sempre che:

1) La legge nazionale identifichi con sufficiente chiarezza le circostanze in cui ciò può avvenire
2) Lo Stato ricevente abbia approntato misure idonee a prevenire abusi e interferenze sproporzionate, ancorché non analoghe a quelle dello Stato mittente
3) Ci siano cautele accentuate per il materiale confidenziale (come quello giornalistico)
4) Ed il trasferimento sia sottoposto a controllo indipendente[31]

Dovendosi però notare sin d'ora, con la promessa di tornarvi nel prosieguo, che tali garanzie attengono alla *trasmissione* dei dati e come tali pongono il problema di quali siano le tutele a salvaguardia della loro *ricezione*.

Chiude la disciplina un'importante postilla. Le tutele finora descritte per i dati di comunicazione vengono infatti estese ai metadati, essendo "non persuasa" la Corte – si

[30] Ibid. §361. *Centrum för Rättvisa*, n. 3 cit., §275.
[31] *Big Brother Watch*, n. 2 cit., §362. *Centrum för Rättvisa*, n. 3 cit., §276.

noti però l'omissione di formule impegnative, in favore di una espressione in termini di dubbio – che la captazione di questi ultimi costituisca una forma di intercettazione necessariamente meno intrusiva della captazione dei primi.[32] Viene così a compiersi, a dispetto della formulazione perfettibile, un'importante equiparazione tra dati e metadati che pone la Corte di Strasburgo in posizione di avanguardia rispetto alla stessa Corte di Lussemburgo, essendo stato rilevato da certa dottrina che quest'ultima, nella sua recente giurisprudenza, avrebbe invece mantenuto un distinguo sul punto, ritenendo in contrasto con il nocciolo duro del diritto alla *privacy* l'accesso generalizzato ai dati, ma non anche quello ai metadati.[33]

Questi, dunque, nel loro complesso, i nuovi parametri individuati dalla CEDU per giudicare la conformità rispetto al diritto alla vita privata delle interferenze generate dalle intercettazioni di massa.

4. L'esame dei casi sub iudice

Passando ora all'applicazione di tali criteri nei casi *sub iudice* è bene procedere ad una lettura sinottica delle due decisioni, avendo questa il pregio di portare alla luce quali differenze di regime hanno ispirato una diversa valutazione della Corte e da ciò potendosi ulteriormente trarre importanti spunti di riflessione sulla fisionomia che a parere dei decisori dovrebbe assumere in concreto un regime di intercettazioni di massa rispettoso del diritto alla vita privata dei cittadini coinvolti. Questo verrà fatto tenendo a mente una piccola differenza: Mentre la legislazione svedese sottopone dati e metadati alle stesse norme, del pari non avviene in Regno Unito. Ne discende che mentre le considerazioni rese dalla CEDU nel caso del *Centrum för Rättvisa* valgono per entrambi, i giudici in *Big Brother Watch* affrontano il tema dei metadati in un apposito paragrafo del quale si darà specifico conto a suo tempo.

4.1. Accessibilità

Ciò detto, e principiando tale analisi dalla "accessibilità" dei rispettivi sistemi può notarsi che in tale ambito non vengono riscontrati particolari problemi: in Svezia la Corte ammette la sussistenza del requisito stante l'assenza di contestazioni sul punto; nel Regno Unito, pur notando la complessità delle fonti, si riconosce che l'introduzione

[32] *Big Brother Watch*, n. 2 cit., §363-364. *Centrum för Rättvisa*, n. 3 cit., §277-278. Si noti che, al contempo, la Corte non richiede che le previsioni legislative che danno forma a tali analogie di tutela presentino formulazione totalmente analoga.
[33] 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. Consultabile presso «https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/». Ultimo accesso eseguito il 22.11.2022.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

a loro chiarificazione del *IC Code* e la natura pubblica di tale documento hanno reso la materia adeguatamente accessibile.[34]

Discorso più articolato riguarda, invece, i canoni della *prevedibilità* e *necessità* dovendosi verificare la corrispondenza delle legislazioni nazionali allo standard in punti descritto al paragrafo precedente.

4.2. I casi in cui le intercettazioni possono essere autorizzate

Lo studio dei casi legittimanti l'uso delle intercettazioni offre un primo esempio del differente approccio con cui ordinamenti differenti disciplinano lo stesso mezzo, posto che, se in entrambi è presente tale indicazione, differente è la tecnica legislativa. Da una parte, il sistema svedese ricorre alla tecnica casistica attraverso una lista in otto punti che, pur nella necessaria astrattezza, identifica altrettanti motivi ispiratori/bersagli delle intercettazioni;[35] il Regno Unito, per contro, ricorre ad una serie di clausole generali secondo cui il Segretario di Stato può emettere un mandato d'intercettazione quando lo ritenga opportuno per ragioni di sicurezza nazionale, per la salvaguardia del benessere economico nazionale o per prevenire o identificare gravi crimini. Per contro, comune ai due sistemi è il solo divieto di usare il frutto delle captazioni nella conduzione dell'azione penale.

Tali divergenze trovano riflesso nella decisione della Corte, poiché mentre l'ordinamento svedese viene promosso a pieni voti, quello britannico viene ammesso con riserva sulla base della genericità dei termini impiegati, che pur non ostando al rispetto dell'art. 8 richiede che tale carenza trovi bilanciamento nel resto del sistema.[36] Da un lato i giudici fissano dunque un paletto, imponendo che i casi d'intercettazione non siano tanto generici da non costringere affatto i poteri dello Stato, e ciò fanno – meritevolmente – ribaltando il giudizio di grado precedente che riteneva i termini

[34] *Big Brother Watch*, n. 2 cit., §365-367. *Centrum för Rättvisa*, n. 3 cit., §279-281.

[35] In particolare, secondo la legislazione svedese, le intercettazioni possono essere condotte per monitorare:

1. Minacce militari esterne al Paese
2. Le condizioni per la partecipazione svedese ad operazioni umanitarie o di *peacekeeping*, o minacce alla sicurezza degli interessi svedesi nello svolgimento di tali operazioni
3. Le circostanze strategiche relative al terrorismo internazionale o ad altri gravi crimini transfrontalieri che possono minacciare gli interessi nazionali
4. Lo sviluppo e proliferazione di armi di distruzione di massa, equipaggiamenti militari e altri specifici prodotti similari
5. Serie minacce esterne alle infrastrutture fondamentali
6. Conflitti esteri con ripercussioni sulla sicurezza internazionale
7. Operazioni di intelligence estera contro gli interessi svedesi, e
8. Le azioni ed intenzioni di una potenza straniera aventi sostanziale importanza per le politiche estere, di sicurezza o difesa svedesi.

Cfr. *Centrum för Rättvisa*, n. 3 cit., §284.

[36] Su tutto quanto riferito vedasi *Big Brother Watch*, n. 2 cit., §368-371. *Centrum för Rättvisa*, n. 3 cit., §284-288.

impiegati nella legislazione britannica sufficientemente puntuali.[37] Dall'altro, però, si ammette che entro certi limiti la carenza così identificata trovi bilanciamento altrove. Sennonché tale ragionamento ha l'effetto collaterale di svilire gli stessi criteri fondamentali da essa individuati, visto che se ogni parametro carente può trovare bilanciamento negli altri, nessuno di questi è essenziale e irrinunciabile. Altresì opinabile è il margine di determinatezza ritenuto bastevole dalla Corte per escludere la violazione (o quantomeno per rendere ancora praticabile un baratto con le altre tutele "fondamentali"). Invero, non si vede come l'abuso del potere di intercettazione possa essere significativamente ristretto da clausole quali la salvaguardia del benessere economico nazionale, potendosi argomentare – come giustamente è stato argomentato – che allora anche lo spionaggio industriale diventa movente sufficiente.[38]

4.3. Le circostanze in cui le comunicazioni di un individuo possono essere intercettate

L'esame delle circostanze legittimanti l'intercettazione delle comunicazioni vede, invece, i due regimi convergere sull'intercettazione delle comunicazioni transfrontaliere, così come nella parallela ammissione dei resistenti che non sempre è agevole distinguere queste dalle comunicazioni puramente interne visto che anche quando mittente e destinatario si trovano sul territorio nazionale, la relativa comunicazione potrebbe essere indirizzata lungo una rete transfrontaliera, così come nel caso in cui si attinga un documento da *servers* posti oltre confine. A ciò si aggiunge, in Svezia, l'ulteriore possibilità che le autorità intercettino le conversazioni nell'ambito delle loro attività di sviluppo che consistono nell'effettuazione di test preliminari sui canali di comunicazione atti a verificarne il valore strategico.[39] Entro tale contesto, dunque, le conversazioni assumono rilievo non tanto per il loro contenuto, quanto per la possibilità che offrono di studiare i sistemi e i percorsi adeguandovi la risposta statale.

Il responso della CEDU, in tutti questi casi, è positivo ma è interessante notarne la motivazione. Pur a fronte dei problemi evidenziati dagli stessi convenuti sulla discriminazione delle comunicazioni interne/esterne, le intercettazioni transfrontaliere

[37] Cfr. *Big Brother Watch* (Prima Sezione), n. 22 cit., §333-335. Come contestato giustamente dalla dottrina, in tale decisione vi è addirittura chi sostiene che i tre, vaghi, criteri britannici sarebbero meglio degli otto svedesi. Vedasi Ibid., *Joint partly dissenting and partly concurring opinion of judges Pardalos and Eicke*, §24, lett. (d); nonchè, I. Cameron, *Regulating signals intelligence*, in *Strasbourg Observers*, 13 luglio 2020. Consultabile presso «https://strasbourgobservers.com/2020/07/13/regulating-signals-intelligence/». Ultimo accesso eseguito il 21.11.2022.

[38] *Big Brother Watch*, n. 2 cit., *Partly concurring and partly dissenting opinion of Judge Pinto De Albuquerque*, §36.

[39] A. LUBIN, *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights*, in *JustSecurity.org*, 2018. Consultabile presso «https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/». Ultimo accesso effettuato il 21.11.2022.

vengono infatti giustificate in Gran Bretagna sulla base dei dichiarati sforzi dell'autorità di limitare tale potere ai soli vettori di informazioni con più alta probabilità di contenere materiale rilevante, in Svezia addirittura *sic et simpliciter*, dal che sembra lecito presumere l'accettazione della Corte dell'inevitabilità di queste catture accidentali, e ciò nonostante le ovvie ricadute sul diritto alla vita privata delle persone coinvolte accidentalmente.

Quanto alle *attività di sviluppo* svedesi, invece, la giustificazione, oltre che nelle cautele predisposte,[40] viene ravvisata sia nella finalità sostanzialmente esplorativa del mezzo – mirante, di principio, ad usare i dati 'grezzi' raccolti a soli fini di adeguamento tecnologico e non di vero e proprio spionaggio – ma soprattutto nella necessità per le autorità di adattare la propria risposta all'evolversi incessante della tecnologia.[41] È dunque la ragion di Stato contemporanea (ossia rapportata alle sfide del presente) a porsi ancora una volta quale vero *leitmotiv* ispirante l'atteggiamento benevolo dei giudici verso la rivisitazione in senso meno garantistico di alcune tutele ritenute in altri momenti innegoziabili: come giustamente notato infatti, nel 1970, la Corte, nel caso *Klass c. Germania* con atteggiamento contrario a quello odierno proibiva espressamente che si potessero svolgere attività di sorveglianza esplorativa in assenza di sospetto.[42] Non può non notarsi, inoltre, che nella misura in cui legittimano la raccolta di dati grezzi ritenendoli non pericolosi, le decisioni odierne pongono la CEDU in linea con la concezione statunitense di *privacy* – secondo cui un'interferenza con tale diritto si verifica al solo momento del trattamento e non anche della raccolta – ma la allontanano dalla sua stessa premessa secondo cui un'interferenza col diritto alla riservatezza si avrebbe in ogni passaggio delle intercettazioni di massa.[43]

4.4. La procedura di autorizzazione

Quanto alle procedure di autorizzazione, se l'ordinamento svedese non pone per la CEDU particolari problematiche – attribuendo tale potere ad un corpo indipendente con approfonditi poteri di vaglio dei canali coinvolti e selettori impiegati[44] – diverso è

[40] Si allude al divieto di usare i dati così acquisiti per generare informazioni di *intelligence* a meno che non rientrino negli 8 casi definiti dalla legislazione svedese (vedi nota 28 *supra*), alla necessità di autorizzazione della *Foreign Intelligence Court*, nonché alla supervisione dell'*Ispettorato*. *Centrum för Rättvisa*, n. 3 cit., §293.
[41] Su tutto quanto riferito nel presente paragrafo vedasi *Big Brother Watch*, n. 2 cit., §372-376. *Centrum för Rättvisa*, n. 3 cit., §289-293.
[42] LUBIN, n. 39 cit. Il precedente riferito è Corte Europea dei Diritti dell'Uomo, Gran Camera, 6 settembre 1978, ricorso 5029/71, *Case of Klass and Others v. Germany*, §51.
[43] Cfr. *Big Brother Watch*, n. 2 cit., §330. Per una più approfondita trattazione dell'argomento vedasi M. CATANZARITI, *La dimensione extraterritoriale della sorveglianza di massa*, in *Rassegna di diritto pubblico europeo*, fasc. 2, 2019, 347 ss.
[44] Secondo il ragionamento della Corte, il potere di autorizzazione è *ivi* assegnato ad un'autorità indipendente, la Foreign Intelligence Court (FIC), il cui presidente e vicepresidenti sono giudici permanenti e i cui membri, pur di nomina governativa, hanno un mandato di durata determinata, nonché

il caso del Regno Unito. È qui, infatti, che la Corte identifica nella dipendenza dall'Esecutivo del Segretario di Stato quale organo incaricato di autorizzare le operazioni e nell'assenza di autorizzazione dei selettori forti,[45] le prime, serie, lacune insormontabili del sistema. E ciò fa rammentando l'imprescindibile valore dell'autorizzazione (indipendente) delle intercettazioni in generale, ma della scelta dei selettori in modo particolare, essendo questi a determinare concretamente quali conversazioni, nel *mare magnum* di dati ottenuti dalle captazioni, formeranno oggetto di concreta analisi.[46] Lacune ancora più gravi quando, come nel caso britannico, riguardano i selettori forti, dato che questi indirizzano la ricerca verso i dati personali di individui specifici.[47] Si consuma così una netta presa di distanza rispetto al giudizio di primo grado, ove tale lacuna era stata ritenuta non produrre, di per sé, alcun contrasto con l'art. 8.[48]

4.5. La procedura di selezione, esame ed uso del materiale intercettato

Il successivo esame delle procedure di selezione, esame ed uso del materiale intercettato risente parzialmente degli esiti dell'analisi precedente. Infatti, nel sistema britannico a formare oggetto di esame è, in ultima analisi, il materiale risultante dall'applicazione dei selettori alla massa aggregata di informazioni raccolte con le intercettazioni, entro cui il certificato del Segretario di Stato identifica le informazioni disponibili agli analisti, sebbene in forma generica. Risulta pertanto evidente che le criticità già esaminate quanto ai selettori, secondo la più tradizionale teoria dell'albero avvelenato, non possono che riflettersi sul materiale che ne costituisce il frutto, così esacerbando i problemi già posti di per sé dalla genericità del certificato del Segretario di Stato. Di tale segno è, appunto, il giudizio della Corte, mentre più benevolo accoglimento viene riservato alle altre procedure in opera che – prevedendo l'accesso solo di personale qualificato, per un periodo di tempo definito, dietro autorizzazione e sottoposte ad audit – vengono ritenute sufficientemente adeguate. Nel complesso,

poteri vincolanti privi di ingerenze governative. Nel chiedere l'autorizzazione di tale corte, l'autorità di intelligence (FRA) è tenuta a specificare l'opportunità dell'operazione in termini di necessita, i canali a cui si richiede accesso e i selettori che si useranno, che dovranno formularsi nella maniera meno intrusiva. Non ultimo, i selettori forti sono sottoposti a cautele rafforzate, dovendo la FIC verificare che il loro uso sia di "eccezionale importanza". Pur prospettandosi dei limiti – in particolare i casi in cui l'esame della corte si riferisca a migliaia di selettori o selettori identificati solo in termini generali – il sistema nel suo complesso viene perciò giudicato accettabile. Cfr. *Centrum för Rättvisa*, n. 3 cit., §296-302.

[45] Nel sistema in discorso sono gli analisti a motivare la scelta dei selettori all'atto del loro inserimento e tale scelta, pur subendo il riesame del *IC Commissioner*, non forma oggetto di specifica autorizzazione nell'ambito del mandato reso dal Segretario di Stato. *Big Brother Watch*, n. 2 cit., §381.

[46] Vedasi *supra* par. 3.

[47] *Big Brother Watch*, n. 2 cit., §377-383.

[48] *Big Brother Watch* (Prima Sezione), n. 22 cit., §381. Sul punto si veda anche G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quaderni Costituzionali*, fasc. 4, 2018, 933.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

dunque, la Corte riacquista la "prudenza" mostrata nell'esame dei primi parametri, non facendo conseguire all'accertamento delle carenze riscontrate il riscontro di una violazione.[49]

Minori problematiche per i giudici pone, ancora una volta, l'ordinamento svedese dove l'unico rilievo mosso attiene alla mancanza di un obbligo di tenere i resoconti delle operazioni svolte sul materiale intercettato, ma tale mancanza non viene ritenuta bastevole ad intaccare la complessiva conformità del regime visto che la sua previsione in circolari interne e l'esistenza di meccanismi di controllo porta i giudici a non dubitare che tali resoconti siano tenuti di fatto, nell'agire concreto degli organi preposti.[50] Motivazione che, francamente, pone più di qualche perplessità, visto che divergendo dalla legge verso la prassi ipotetica, si finisce per rimettere il rispetto dei diritti delle galline (leggasi: i cittadini) alla buona volontà del lupo (leggasi: gli Stati), per di più presunta.[51]

4.6. La condivisione del materiale con terze parti

In ogni caso, la situazione sopra descritta si capovolge passando all'esame dei regimi di trasmissione dei dati, perché se qui è il sistema britannico a risultare adeguato allo standard CEDU,[52] per la prima volta la Corte accerta una significativa carenza del sistema svedese; data non tanto dal circolo di autorità domestiche con cui può avvenire la condivisione – sufficientemente circoscritto – quanto dall'eccessiva genericità della legge che permette al FRA di condividere dati ogniqualvolta lo ritenga conforme all'interesse nazionale, in uno con l'assenza di un espresso requisito che nel far ciò si ponderi la necessità e proporzionalità dello scambio o si accerti se il ricevente ha in atto sufficienti tutele.

Più nel dettaglio, è interessante notare che nell'ambito di tale decisione i giudici riconoscono che un certo margine di indeterminatezza nell'identificare le circostanze legittimanti lo scambio sia inevitabile, tenuto conto che l'imprevedibilità delle situazioni che possono portare alla cooperazione tra Stati rende poco opportuno ingessarla in una tassativa lista di ipotesi, ma al contempo viene richiesto che le disposizioni siano pur sempre tali da limitare i rischi di abusi o interferenze

[49] *Big Brother Watch*, n. 2 cit., §384-391.
[50] *Centrum för Rättvisa*, n. 3 cit., §303-316.
[51] Tale perplessità, peraltro, può estendersi a buona parte delle pronunce visto che è la Corte stessa a dare atto di svolgere un'analisi dei regimi portati alla sua attenzione sulla base di informazioni limitate. Cfr. *Big Brother Watch*, n. 2 cit., §323; *Centrum för Rättvisa*, n. 3 cit., §237.
[52] Essendo previsto a livello interno che la divulgazione del materiale intercettato avvenga nei confronti del minor numero di persone, sia necessario e le persone informate abbiano bisogno di ricevere tali dettagli per svolgere i propri compiti istituzionali (c.d. need-to-know principle); mentre, a livello esterno, l'accertamento che il ricevente abbia in opera sufficienti tutele, che la divulgazione sia effettuata nei suoi confronti nella minima estensione necessaria e venga richiesto nei casi di dubbia liceità il parere di un esperto. Cfr, *Big Brother Watch*, n. 2 cit., §392-399.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

sproporzionate. Non è quindi la genericità della legge svedese in sé la causa ultima della decisione della Corte, quanto il fatto che a questa non facciano da contraltare adeguate considerazioni del diritto alla vita privata delle persone coinvolte;[53] scelta che a dispetto di altre oggetto di precedenti dubbi sembra potersi condividere, mirando ad attribuire agli Stati un certo margine operativo pur non risolvendosi in un'acritica compressione dei corrispettivi diritti dei cittadini. Tale decisione marca, inoltre, un evidente passo avanti rispetto all'approccio adottato dalla Prima Sezione, che pur rilevando la genericità delle previsioni legislative ed il potenziale effetto negativo sui diritti dei cittadini aveva fatto salvo il regime svedese, così sollevando le critiche della dottrina.[54]

4.7. I limiti di durata delle intercettazioni, di conservazione del materiale e le circostanze in cui questo materiale può essere cancellato o distrutto

Decisamente meno controverse risultano, in ogni caso, le previsioni dedicate dagli Stati resistenti alla durata delle intercettazioni così come alla conservazione e distruzione del relativo materiale, generalmente giudicate sufficientemente chiare ed efficaci, con la sola eccezione della rilevata assenza nel sistema svedese di previsioni disciplinanti la distruzione di materiale non personale. Norma che, a parere della Corte, dovrebbe essere presente nei casi in cui il mantenimento di tali dati può pregiudicare il diritto alla riservatezza della corrispondenza, fissando come criterio minimo l'obbligo di distruzione del materiale non più rilevante a fini di intelligence, ma la cui mancanza nel caso di specie non dà luogo a condanna, trovando compensazione nella complessiva bontà del sistema. In tale campo i giudici tornano, dunque, a compiere quell'opera di bilanciamento tra salvaguardie minime che si è già avuto modo di constatare (ed in parte contestare) in alcuni passaggi precedenti.[55]

4.8. La supervisione delle operazioni

Del pari positivo è il giudizio della Corte sui mezzi di supervisione delle intercettazioni approntati dai convenuti, vale a dire le procedure e modalità con cui

[53] Su tutto quanto riferito nel presente paragrafo vedasi *Centrum för Rättvisa*, n. 3 cit., §317-330. Sostegno dell'ultimo argomento si ricava, tra l'altro, dall'affermazione della Corte in *Big Brother Watch*, n. 2 cit., §395, laddove questa afferma che: "il trasferimento di materiale a partner d'intelligence stranieri o organizzazioni internazionali darebbe luogo a problemi sotto il versante dell'art. 8 se lo Stato intercettante non si assicurasse dapprima che il partner, nel maneggiare il materiale, abbia in opera tutele capaci di prevenire abusi o interferenze sproporzionate".
[54] LUBIN, n. 39 cit.
[55] Si allude a quanto detto *supra, § 4.2*. Su tutto quant'altro riferito nel presente paragrafo vedasi *Centrum för Rättvisa*, n. 3 cit., §§331-344. *Big Brother Watch*, n. 2 cit., §§400-405.

l'autorità indipendente monitora il rispetto dei parametri precedenti e i suoi poteri in caso di violazione.

In particolare, in Svezia, i giudici si dicono persuasi dell'indipendenza dell'autorità preposta al controllo, il *Foreign Intelligence Inspectorate* (FII), i cui membri sono selezionati per un mandato di 4 anni tra i candidati proposti dai gruppi parlamentari, e il cui comitato di presidenza è composto da giudici permanenti o ex giudici. Come del pari soddisfacenti vengono ritenuti i poteri dell'Ispettorato, potendo nella maggior parte dei casi ordinare la cessione delle operazioni e la distruzione del relativo materiale, in alcuni casi ricorrere alle autorità dotate dei poteri vincolanti di cui è sprovvisto ed in altri casi ancora rendere raccomandazioni che, quand'anche non vincolanti, nella prassi risultano puntualmente recepite dall'autorità d'intelligence.[56]

Simile accoglimento, nel Regno Unito, riceve l'IC *Commissioner* che, nominato tra persone aventi precedentemente ricoperto alti ruoli giudiziari e dotato del potere di segnalare le irregolarità riscontrate al primo ministro e alle autorità coinvolte (compiti regolarmente svolti) ricevendo riscontro delle migliorie apportate, viene ritenuto fornire dai giudici un controllo sufficientemente indipendente ed efficace.[57]

In entrambi i casi, però, non si possono non manifestare alcune perplessità, dovendosi notare da un lato che l'Ispettorato svedese non appare pienamente svincolato dal governo, essendo questo ad eleggere i suoi membri e per un termine inidoneo a garantirgli piena indipendenza; dall'altro, che il Commissario britannico non sembra costituire un rimedio efficace, visto che gran parte dei suoi poteri consistono nella sottoposizione di report allo stesso esecutivo.[58]

4.9. Il controllo post fatto

Terminato l'esame dei mezzi di supervisione, ambito finale d'analisi della Corte diventa quello degli strumenti di controllo post fatto, compito che la legislazione britannica assegna all'*Investigatory Powers Tribunal* (IPT), e la legislazione svedese al *Foreign Intelligence Inspectorate*.

Si è, dunque, in presenza di un evidente peculiarità, perché mentre nel Regno Unito titolare del potere è un organo distinto dall'*IC Commissioner* che svolge la supervisione in corso d'opera, in Svezia il controllo post fatto è assegnato alla stessa autorità incaricata della fase precedente. Proprio tale caratteristica ispira il ragionamento della Corte che, notando come la sua duplicità di ruoli possa portare in alcuni casi – e con evidente conflitto d'interessi – l'Ispettorato a diventare giudice della

[56] *Centrum för Rättvisa*, n. 3 cit., §§345-353.
[57] *Big Brother Watch*, n. 2 cit., §§406-412.
[58] Quest'ultimo argomento forma anche parte dell'opinione dissenziente del Giudice Pinto De Albuquerque, *Big Brother Watch*, n. 2 cit., *Partly concurring and partly dissenting opinion of Judge Pinto De Albuquerque*, §47.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

propria opera, ravvisa in tale impianto una seconda sostanziale carenza dell'ordinamento svedese, aggravata dal fatto che tale sistema di revisione non dà luogo a decisioni motivate.[59]

Per contro l'IPT inglese viene giudicato un mezzo efficace ed indipendente, ragionando la CEDU che questo risulta dotato di pervasivi poteri di esame non dipendenti dalla notifica ai soggetti coinvolti (che possono perciò ricorrervi al semplice sospetto di essere stati intercettati), nonché del potere in caso di violazione di indennizzare le persone lese ed emanare ogni altro ordine resosi necessario.[60] Il problema evidenziato quanto a questa impostazione è solo uno: e cioè che un organo che agisce solo su richiesta dei soggetti che si ritengono lesi rappresenta una tutela solo teorica per chi non sospetta di essere stato intercettato.[61] Obiezione che non si può che condividere, sembrando ben più rispettoso dei diritti umani coinvolti un sistema che, sul modello dell'obbligo dell'azione penale nostrano prevedesse, accanto alla richiesta individuale, l'indagine d'ufficio sulla liceità delle intercettazioni svolte. Nondimeno si deve riconoscere a tale parte dell'analisi il compito di individuare due importanti cautele: *in primis*, la necessaria terzietà dell'organo di controllo successivo rispetto all'organo di controllo simultaneo, dall'altra l'importanza che assume nello svolgimento di tale compito l'obbligo di motivazione, poiché è solo in base a questa che i consociati sono posti nella condizione di comprendere il modo in cui la legge è stata applicata ed eventualmente sindacarlo.

4.10. I relativi metadati

A margine dell'analisi generale, permane, per il solo Regno Unito, l'esame delle considerazioni rese dalla Corte EDU sul locale regime di trattamento dei metadati. Se il regime svedese si sottrae a questo ulteriore passaggio per la totale identità di previsioni governanti i due ambiti, deve osservarsi che pure nel caso del Regno Unito l'esame della Corte muove dalla constatazione che la legislazione dei metadati è in gran parte coincidente con quella dei dati di comunicazione, potendosi perciò applicare ad essa le stesse considerazioni – ed accertamenti di violazione – rese in quel caso.

Due sole differenze formano oggetto di distinguo: da un lato la circostanza che, sottraendosi al regime di cui all'art. 16(2) del RIPA (acronimo di *Regulation of Investigatory Powers Act*, ossia il testo disciplinante l'esercizio dei poteri di intercettazioni di massa nel Regno Unito), la scelta dei metadati da parte degli analisti non deve essere giustificata in termini di necessità e proporzionalità; dall'altro il fatto che i metadati non corrispondenti ad alcun selettore non sono immediatamente cancellati bensì conservati per diversi mesi.

[59] *Centrum för Rättvisa*, n. 3 cit., §§354-364.
[60] *Big Brother Watch*, n. 2 cit., §§413-415.
[61] *Big Brother Watch*, n. 2 cit., *Partly concurring and partly dissenting opinion of Judge Pinto De Albuquerque*, §49.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Tali differenze non vengono però ritenute dar luogo a problemi significativi, attenendo ad aspetti secondari.[62] Ancora una volta, ed in analogia con l'opinione resa in sede di dati di comunicazione, il problema fondamentale resta, dunque, la mancata autorizzazione indipendente dei selettori forti.[63]

4.11. Le conclusioni della Corte

Punto terminale del ragionamento della CEDU è, in entrambi i casi, l'accertamento di una violazione del diritto alla vita privata dei cittadini fondata sull'assenza, nel Regno Unito, di autorizzazione indipendente delle intercettazioni e dei relativi selettori forti e, in Svezia, di sufficienti garanzie nella condivisione dei dati e di un'autorità indipendente di controllo successivo.

5. Il diritto alla libertà di espressione

Problema complementare ma distinto è quello della conformità delle intercettazioni di massa con il diritto alla libertà di espressione tutelato dall'art. 10 della Convezione Europea dei Diritti dell'Uomo, esaminato però dalla Corte nell'ambito del solo caso *Big Brother Watch* ed in relazione ai soli giornalisti (essendo risultato inammissibile il ricorso delle NGO per mancato esaurimento dei rimedi domestici).[64]

Qui, centrale nel ragionamento della Corte è la considerazione dell'importanza che la protezione delle fonti giornalistiche assume per la libertà di stampa quale peculiare manifestazione della libertà di espressione, atteso che, senza tale protezione, tali fonti potrebbero essere dissuase dal condividere le informazioni in loro possesso, ed il ruolo della stampa quale "cane da guardia" dell'interesse pubblico contro gli abusi dei governanti risulterebbe evidentemente compromesso.[65] Perciò, la decisione della Corte passa attraverso l'identificazione dei canoni che giustificano l'interferenza con il diritto alla riservatezza delle fonti giornalistiche. A tal proposito, l'opinione dei giudici è che tale interferenza sia conforme a Convenzione solo laddove motivata da imperative ragioni di interesse pubblico e assistita da adeguate cautele, prima tra tutte la presenza di un giudice o altro organismo indipendente dotato del potere di accertare la ricorrenza

[62] Anzi, riconoscendo l'importanza che i metadati hanno per i governi nel contrasto al terrorismo, la Corte accetta l'obiezione di quest'ultimo circa la scarsa opportunità di estendervi le tutele dell'art. 16(2) RIPA, tenuto conto della mole di questi e dell'importanza di processarli immediatamente, cosa che evidentemente diverrebbe impossibile laddove ci si dovesse premurare di giustificarne necessità e proporzionalità. Allo stesso modo viene accettata la giustificazione che la conservazione dei metadati per un lungo periodo si rende necessaria per i lunghi tempi di analisi che questi richiedono. Cfr. *Big Brother Watch*, n. 2 cit., §§421-423.
[63] Su tutto quanto riportato vedasi *Big Brother Watch*, n. 2 cit., §§416-423.
[64] *Big Brother Watch*, n. 2 cit., §428.
[65] Ibid. §442.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

di tali presupposti ed eventualmente impedire quegli accessi inutili che potrebbero compromettere la riservatezza delle fonti. Nondimeno, una fondamentale linea di demarcazione tra le fattispecie viene tracciata tra il caso in cui le autorità ordinino al giornalista di rivelare le proprie fonti ed il caso in cui, per svelare l'identità di queste ultime, si effettuino ricerche direttamente a casa sua o sul suo luogo di lavoro, visto che qui l'accesso, quand'anche improduttivo, fornisce visione di tutti i documenti del giornalista, così dando vita ad un'intrusione significativamente maggiore della precedente.[66]

L'opera della Corte, però, non si arresta alla identificazione di principi generali, perché, analogamente a quanto fatto in relazione al diritto alla vita privata, alla delineazione di tale quadro fa seguito ancora una volta l'adattamento dello stesso alla peculiarità delle intercettazioni di massa, cosa che nel caso di specie viene fatta creando una importante analogia. L'interferenza occasionata da intercettazioni di massa dirette a svelare fonti giornalistiche viene, infatti, equiparata a quella che si avrebbe nel caso della perquisizione presso la sua casa o luogo di lavoro, richiedendosi che i selettori impiegati a tal fine siano autorizzati da un'autorità indipendente (o giudice) dotata del potere di verificare l'esistenza di ragioni imperative di interesse pubblico e la fattibilità di mezzi meno invasivi. Caso differente viene invece ritenuto quello delle intercettazioni non dirette alle fonti giornalistiche in cui queste vengano captate accidentalmente, visto che qui, chiaramente, non può avvenire un controllo *a priori* sulla necessità dell'interferenza o la presenza di mezzi meno invasivi e tale controllo deve perciò avvenire una volta che ci si sia accorti dell'errore e si voglia continuare ad usarle.[67]

È il caso di evidenziare che queste cautele non scalzano quelle precedentemente individuate con riguardo alla tutela della vita privata ma costituiscono una loro specificazione giustificata dal particolare valore assegnato alla salvaguardia della libertà di stampa/espressione. Ne consegue, che in quanto ipotesi a tutela speciale, a maggior ragione il regime intercettivo risulterà carente nei confronti dei giornalisti se già risulta carente nei confronti dei *quivis de populo*, beneficiari delle tutele "standard".

In questo quadro – e passando ora all'esame della decisione del caso *sub iudice* – poco conta per i giudici di Strasburgo che il Regno Unito preveda cautele aggiuntive per le fonti giornalistiche,[68] perché le deficienze riscontrate nel regime ordinario sono già tali da compromettere la tenuta del sistema nel suo complesso e risultano peraltro enfatizzate dall'assenza di un'autorità indipendente dotata del potere di valutare, nei

[66] Ibid. §§443-444.
[67] Ibid. §§448-450.
[68] In particolare, ogni richiesta di mandato deve dichiarare il rischio di violazioni collaterali della privacy – inclusa quella dei giornalisti – specificando, ove possibile, le misure da prendersi per ridurre il rischio di intrusioni anche se tale cautela viene riferita alle sole intercettazioni mirate. Allo stesso modo, quando scopo delle intercettazioni è acquisire informazioni personali confidenziali, viene previsto l'obbligo di indicare ragioni, necessità e proporzionalità della scelta anche se la dizione "informazioni personali confidenziali" sembra indicare qualcosa di distinto dal "materiale confidenziale giornalistico". Cfr. ibid. §§453-454.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

termini di cui si è detto, l'impiego di selettori forti riferiti ai giornalisti o la sussistenza di sufficienti ragioni per mantenerne i dati intercettati una volta che divenga chiara la loro acquisizione accidentale. Ne discende un accertamento di violazione anche in ordine all'art. 10 CEDU.[69]

6. La ricezione di informazioni da servizi d'intelligence estera

Ultimo aspetto delle intercettazioni di massa ad essere esaminato nel caso *Big Brother Watch* è la ricezione di informazioni da servizi d'intelligence estera.

In tale campo l'esame della Corte inizia con l'identificazione di un criterio procedurale: per potere rivestire la qualità di vittime – e quindi avere *jus standi* – sulla base della mera esistenza di un sistema di sorveglianza di massa, ai ricorrenti viene infatti chiesto di dimostrare di essere stati potenzialmente a rischio che il Regno Unito venisse in possesso delle loro comunicazioni tramite richiesta ad un'agenzia d'*intelligence* estera.[70]

Il principio di base in ambito "sostanziale" viene invece identificato dai giudici in un assunto logico: e cioè che la protezione garantita dalla CEDU diverrebbe effimera se agli Stati fosse dato aggirare i loro obblighi attraverso la richiesta di informazioni d'*intelligence* a servizi stranieri. Che la Corte sviluppi bene le conseguenze di tale affermazione è, però, quantomeno dubbio. Si richiede che la richiesta di informazioni abbia una base nella legislazione domestica, che tale legge sia accessibile e prevedibile, che ci siano chiare indicazioni ai cittadini sulle circostanze e condizioni di tale richiesta, che ci siano sufficienti tutele contro il rischio di elusione, così come per l'uso ed immagazzinamento di tali dati, ma nulla si dice dello Stato mittente.[71] Soprattutto, il modo in cui questo sia entrato in possesso dei dati che si appresta a trasmettere rimane fuori dal perimetro della Corte, né questa pretende che gli Stati riceventi ottengano tali informazioni prima della consegna. Perciò, nessuno assicura che nel carpire i dati lo Stato trasmittente – non CEDU – abbia assunto cautele analoghe a quelle che vengono richieste al membro CEDU sul piano interno (si pensi, solo per fare un esempio tra i più significativi, alla necessità di autorizzazione indipendente dei selettori forti). Come efficacemente evidenziato, proibire astrattamente l'elusione non basta, bisogna fissare dei meccanismi per assicurare che ciò non avvenga in pratica.[72] Per contro, per la Corte, il trasferimento di materiale *a* l'estero deve essere sottoposto a controllo indipendente,

[69] Ibid. §§451-458.
[70] Cosa che, nel caso di specie, viene desunta dalle dichiarazioni dell'IPT rese nel caso *Liberty* secondo cui le conversazioni di due dei ricorrenti erano state trattenute, ciò implicando che queste avevano corrisposto un selettore forte e come tali potevano aver formato oggetto di captazione dell'NSA americana visto che questa, al tempo, usava simili selettori. Ibid. §§468-469. Per il resto del discorso vedasi invece ibid. §§467-472.
[71] Ibid. §§497-499.
[72] *Big Brother Watch*, n. 2 cit., Joint partly dissenting opinion of judges Lemmens, Vehabović, Ranzoni and Bošnjak, §8.

ma non la sua ricezione *da* l'estero.[73] Peggio ancora, le cautele individuate si applicano solo al materiale che gli Stati stessi (sic!) identificano come provento delle intercettazioni,[74] con una procedura logica non dissimile da quella che si avrebbe chiedendo all'evasore di essere lui stesso ad identificare i propri beni da sottoporre a tassazione. Si tratta, con tutta evidenza, di un approccio sensibilmente diverso da quello fatto proprio dalla Corte di Giustizia dell'Unione Europea che, invece, pone al centro della valutazione anche le cautele predisposte dallo stato estero, come nel caso *Schrems II* dove a determinare la bocciatura dell'accordo Europa-Stati Uniti era proprio l'assenza di sufficienti garanzie nel regime di sorveglianza d'oltreoceano.[75]

In virtù del riferito approccio della Corte, non sorprende che l'analisi del regime britannico non dia luogo a rilievi di sorta: la base legale viene trovata nell'accordo per lo scambio di dati *d'intelligence* Stati Uniti-Gran Bretagna del 1946, giudicato adeguatamente accessibile dopo l'incorporazione nell'*IC Code*; le circostanze e condizioni dello scambio vengono ritenute conformi, applicandosi ad esse lo stesso regime già ritenuto compatibile con le intercettazioni interne; perfino l'autorizzazione della richiesta di trasmissione viene giustificata sulla base della sua provenienza dal Segretario di Stato (quello stesso Segretario di Stato che sul piano interno era stata ritenuto inidoneo ad approvare le operazioni); allo stesso modo soddisfacenti vengono ritenute le disposizioni previste per l'esame, uso e immagazzinamento dei dati, così come la protezione offerta dall'*IC Commissioner* prima e dall'*IPT* dopo.[76]

Il pronosticabile esito è la conformità del regime esaminato agli artt. 8 e 10 della Convenzione.

7. Considerazioni a margine delle sentenze

Così terminata l'analisi, appare interessante guardare all'eco che le pronunce hanno avuto tra società civile e dottrina, traendo dai contenuti di tale dibattito eventuali spunti di riflessione.

In tal prospettiva è interessante notare, anzitutto, che mentre le associazioni per i diritti civili hanno spesso salutato le decisioni della Gran Camera come una vittoria della *privacy*,[77] la dottrina si attesta su posizioni ben più caute, ravvisandovi, semmai,

[73] *Big Brother Watch*, n. 2 cit., *Partly concurring and partly dissenting opinion of Judge Pinto De Albuquerque*, §51.
[74] Ibid. §53.
[75] M. ZALNIERIUTE, *Big Brother Watch and Others v. the United Kingdom*, in *American Journal of International Law*, vol. 116(3), 2022, 589. Sulla sentenza si veda anche R. BIFULCO, i*l trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno,* in *Diritto Pubblico Europeo: Rassegna online*, vol. 2, 2020, 1-17.
[76] *Big Brother Watch*, n. 2 cit., §§500-513.
[77] Così, ad esempio, Privacy International ed Amnesty international, ricorrenti nel processo *Big Brother Watch.* Cfr. *Human rights groups win European Court of Human Rights claim on UK mass surveillance regime*, in *privacyinternational.org*. Consultabile presso «https://privacyinternational.org/press-

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

l'istituzionalizzazione delle intercettazioni di massa.[78] Deve infatti rilevarsi che l'argomento principe delle ONG – per cui le intercettazioni di massa costituirebbero interferenze indefettibilmente sproporzionate – nelle pronunce odierne risulta essenzialmente soccombente a fronte dell'accertamento di lacune minime che, come qualcuno ha notato, possono essere sanate senza alterare sostanzialmente i sistemi di sorveglianza coinvolti.[79] Conferma autoritativa di ciò si ravvisa, oltre che nell'impianto argomentativo delle stesse decisioni, anche nell'audizione davanti al parlamento del Segretario di Stato britannico all'indomani delle due pronunce, ove questi, prima ancora di dare atto dei problemi riscontrati e delle misure in corso d'adozione, tiene a rimarcare che la Corte ha preso atto della cruciale importanza delle intercettazioni di massa, escludendo che queste siano categoricamente contrarie alla Convenzione![80]

Strettamente connesso con l'argomento dell'istituzionalizzazione delle intercettazioni di massa è il tema del discostamento che tali pronunce marcano tra la giurisprudenza CEDU e CGUE (con tale acronimo intendendosi la Corte di Giustizia dell'Unione Europea) in tema di diritto alla riservatezza, prima convergente. Invero, tali corti hanno proceduto per diverso tempo lungo un percorso parallelo caratterizzato da una crescente tutela accordata al diritto alla riservatezza.[81] Rispetto a tale quadro, le pronunce odierne appalesano per certi versi un'inversione di tendenza, consistente in

release/4522/human-rights-groups-win-european-court-human-rights-claim-uk-mass-surveillance». Ultimo accesso effettuato il 23.11.2022. Su posizioni più moderate si attesta invece l'International Commission of Jurists (ricorrente nello stesso caso), che infatti parla di decisione epocale che disattende le aspettative. M. FRIGO, *Big Brother Watch v. UK: A Landmark Judgment Missing the Mark*, in *Voelkerrechtsblog*. Consultabile presso «https://voelkerrechtsblog.org/big-brother-watch-v-uk/». Ultimo accesso effettuato il 23.11.2022.

[78] Si veda, ad esempio, 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*. Consultabile presso «https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/». Ultimo accesso eseguito il 23.11.2022.

[79] F. DUBUISSON, *La Cour Européenne des Droits de l'Homme face à la surveillance de masse*, in *Revue trimestrielle des droits de l'Homme*, vol. 1, 2022, 125.

[80] UK Parliament, House of Commons, 31 marzo 2022, written statement of The Secretary of State for the Home Department, *Grand Chamber ECtHR Judgment in Big Brother Watch and Others v. UK*. Consultabile presso «https://hansard.parliament.uk/Commons/2022-03-31/debates/22033139000028/GrandChamberEcthrJudgmentInBigBrotherWatchAndOthersVUK».

[81] Volendo brevemente ripercorrere le tappe della vicenda, questa ha inizio, sul versante strasburghese, con il caso *Weber*, in cui pur non accertandosi violazioni venivano fissati i criteri in materia di misure di sorveglianza. Il caso *Liberty* confermava gli esiti dell'analisi precedente, mentre con i casi *Roman Zakharov* e *Szabó e Vissy* si compivano altrettanti passi avanti nella protezione del diritto alla riservatezza introducendo, rispettivamente, il requisito del ragionevole sospetto e quelli dell'autorizzazione giudiziaria e successiva notifica. Sul versante belga, invece, la CGUE iniziava ad occuparsi della sorveglianza di massa nel caso *Digital Rights Ireland* statuendo la necessità di regole precise e cautele minime, negando al contempo che la lotta al crimine fosse una giustificazione sufficiente a permettere intercettazioni generalizzate. Tali conclusioni venivano successivamente riprese nel caso *Tele2*, in cui ad esse si aggiungevano i requisiti della stringente necessità, della previa autorizzazione indipendente e della notifica. Per una trattazione più estensiva sul punto e puntuali rimandi alle pronunce citate si rinvia a V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, in NATIONAL RESEARCH UNIVERSITY: HIGHER SCHOOL OF ECONOMICS, *Basic Research Program Working Papers*, series: law, wp brp 87/law/2019, 1-10.

una maggiore attenzione dei giudicanti verso le necessità dei governanti e nella corrispondente erosione di alcune garanzie a favore dei governati, quali i requisiti del ragionevole sospetto e della notifica.[82] Tale decisione della Gran camera si pone in continuità con quella della Camera semplice ma segna, appunto, una netta rivisitazione del precedente approccio della Corte in tema di misure di sicurezza. L'interrogativo che ne nasce è, dunque, se tale mutamento debba attribuirsi alla necessità di adattare il diritto esistente ai tratti innovativi della nuova fattispecie onde salvaguardarne la forza precettiva ovvero sia il frutto di un vero e proprio ripensamento da parte della Corte sull'opportunità di garantire agli stati un maggiore margine d'azione, in parte svincolato dalle peculiarità del caso di specie; e se, in tal caso, il mutato atteggiamento sia a sua volta – come sostenuto da qualcuno – espressione di un maggior favore della Corte verso i paesi occidentali (le pronunce più restrittive vedevano infatti coinvolti paesi dell'Europa orientale) sul presupposto che la loro forma democratica di governo sia già di per sé una garanzia dagli abusi.[83] Evidentemente, qualsivoglia risposta al precedente interrogativo sarebbe destinata a rimanere in buona misura puramente congetturale, perciò si lascia alla sensibilità del lettore. Comunque si risolva il dilemma è, però, interessante notare la coeva scelta della CGUE, nel caso *Quadrature du Net*, di rivedere la propria giurisprudenza in tema di conservazione dei dati in senso meno garantistico rispetto al coinvolto diritto alla riservatezza, ammettendone la ritenzione indiscriminata laddove questa si renda necessaria per ragioni di sicurezza nazionale.[84] Alcuni hanno ravvisato in tale pronuncia una convergenza tra le due corti in direzione di una maggiore valorizzazione delle esigenze di sicurezza nazionale nell'ambito del bilanciamento con il diritto alla riservatezza. Per altri, invece, il caso marcherebbe una divergenza più che una convergenza, posto che a dispetto della CEDU, la CGUE avrebbe comunque qualificato le ragioni securitarie come un'eccezione alla regola attorniandole di un quadro di rigorose garanzie e non, invece, istituzionalizzandole.[85] Ciò che si vede, in ogni caso, è che, lungi dal trovare risposta definitiva, l'interrogativo sui motivi ispiranti il mutato approccio al diritto alla riservatezza emerge in più punti del dibattito contemporaneo; quale segno, forse, di comuni incertezze tra le corti e la dottrina su punto in cui fissare lo scomodo bilanciamento tra sicurezza nazionale e diritti umani coinvolti.

---

[82] Ibid. 11.
[83] B. VAN DER SLOOT, E. KOSTA, n. 16 cit., 258.
[84] M. ZALNIERIUTE, n. 75 cit., 591. La decisione riferita è, Corte di Giustizia dell'Unione Europea, Grande Camera, 6 ottobre 2020, Cause C 511/18, 512/18, C 520/18, *La Quadrature du Net e a. contro Premier ministre e a*. Consultabile presso «https://curia.europa.eu/juris/document/document.jsf;jsessionid=92544B98822139C2F681CA3C92D81381?text=&docid=232084&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=1940482».
[85] V. SIZAIRE, *L'art du trompe-l'œil. À propos des arrêts du 25 mai 2021, Big brother watch et autres c. Royaume-Uni et Centrum för Rättvisa c. Suède de la Cour européenne des droits de l'homme*, in *La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux*., 2021, 1.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Similmente, la comparazione tra la giurisprudenza CEDU e CGUE in tema di tutela della sicurezza nazionale pone in evidenza un altro aspetto delle decisioni ora in esame su cui diversa dottrina si è concentrata: vale a dire la mancata specificazione, da parte della Corte, di alcuni canoni da essa individuati. Se è vero, infatti, per come si è detto, che entrambi le corti europee ancorano adesso alla sussistenza di preminenti ragioni di sicurezza nazionale la liceità di misure invasive del diritto alla riservatezza, è vero anche che la CEDU lascia totalmente alla discrezionalità statale l'identificazione del ricorrere di tali esigenze mentre la CGUE sembra compiere uno sforzo ulteriore, identificando a presupposto delle più gravose misure il sussistere di "una minaccia grave per la sicurezza nazionale che si riveli reale e attuale o prevedibile".[86] Certamente è lecito dubitare di quale sia l'effettiva portata garantista di un concetto così flessibile quale quello di prevedibilità ma è quantomeno lodevole che i giudici di Lussemburgo abbiano profuso un maggiore sforzo nell'accostarsi ai tratti peculiari del fenomeno in esame, cercando di porne una regolamentazione quanto più puntuale e non lasciandone la definizione alla discrezionalità degli Stati (ossia degli stessi soggetti che dovrebbero essere costretti da quelle norme) così come fatto dalla Gran Camera.

Non ultimo, vi è il tema (del mancato esame) della efficacia extraterritoriale della Convenzione EDU e dei relativi diritti.[87] Com'è agevole notare, infatti, le intercettazioni di massa sono strutturalmente extraterritoriali, bersagliando una platea potenzialmente enorme di persone locate fuori dal territorio dello Stato intercettante e i cui dati transitano anch'essi su canali internazionali.[88] Una decisione sul punto sarebbe perciò stata quantomai opportuna. La Corte, invece, schiva elegantemente il problema sulla base della mancata eccezione di giurisdizione territoriale da parte dei convenuti, dicendo, cioè, che in assenza di contestazioni sul punto, l'analisi avrebbe mosso dall'assunto che i fatti in contestazione rientrassero nella competenza degli Stati.[89] Sulla base di questo solo dato si potrebbe forse sostenere che pur non sancendo una vera e propria applicazione extraterritoriale della Convenzione la Corte abbia implicitamente aderito ad una nozione particolarmente ampia di giurisdizione, di fatto estendendola

[86] Corte di Giustizia dell'Unione Europea, *La Quadrature du Net*, n. 84 cit., §137. Cfr. anche V. SIZAIRE, *Savoir resserrer les mailles du filet à propos de l'arrêt du 6 octobre 2020 de la Cour de Justice de l'Union Européenne*, in *La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux*., 2020, 2.

[87] Per una estensiva analisi del tema dell'applicazione extraterritoriale dei trattati si veda M. MILANOVIC, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal*, vol. 56, n. 1, 2015, 81-146.

[88] Cfr. M. CATANZARITI, n. 43 cit., 340.

[89] Si allude a *Big Brother Watch*, n. 2 cit., §272, secondo cui: *«In respect of the section 8(4) regime, the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the Government expressly confirmed that they had raised no objection on this ground as at least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the section 8(4) regime, the matters complained of fell within the jurisdictional competence of the United Kingdom».*

oltre i confini nazionali; ma resta il fatto che una espressa statuizione sul criterio radicante la giurisdizione manca. Finora – con ciò intendendosi prima delle pronunce odierne – la Corte ha legato l'applicazione delle norme convenzionali al difuori dei confini degli Stati membri al criterio "territoriale" del controllo effettivo da questi esercitato su un territorio estero, da solo o congiuntamente al criterio "personale" dell'esercizio da parte dello Stato membro di autorità o controllo sulle vittime dei suoi atti, non ritenendo però bastevole a fondare la giurisdizione tale criterio solamente[90] e ravvisando, per giunta, la sussistenza di un nesso personale solo in atti statali particolarmente invasivi, quali la capacità di uccidere i civili stranieri.[91] Il problema è che durante le intercettazioni di massa lo Stato intercettante non esercita controllo sul territorio in cui risiede il bersaglio – tanto più che spesso le intercettazioni avvengono all'insaputa o addirittura contro le autorità locali[92] – salvo non ammettere, nel caso di uso della potestà statale in forma immateriale, che la violazione si collochi spazialmente non (o quantomeno non solo) nel territorio in cui l'azione integrante la violazione colpisce i soggetti passivi, nel nostro caso gli intercettati, ma laddove questa viene posta in essere dai suoi soggetti attivi, vale a dire gli intercettanti. Cosa che però non risolverebbe il problema dell'extraterritorialità ma semplicemente ricondurrebbe l'azione entro una nozione estesa di territorio statale. Tantomeno lo stato intercettante esercita un controllo sui soggetti passivi, visto che per sua definizione la sorveglianza segreta è tanto più efficace quanto meno gli intercettati percepiscono lo svolgersi dell'azione. Perciò, pur volendo fare uno sforzo ermeneutico atto a ricavare dalla precedente giurisprudenza CEDU la vigenza autonoma del criterio personale, sarebbe tutt'altro che agevole ricondurvi le intercettazioni di massa posto che la sua sussistenza è stata sempre radicata nell'uso materiale della forza. Come si vede, quindi, un intervento chiarificatore della Corte sarebbe stato – e rimane – quantomai opportuno, apparendo particolarmente preoccupante che in un caso sulla protezione di diritti e libertà fondamentali di una platea potenzialmente vastissima di persone rimanga

[90] Si pensi, quale esempio di applicazione particolarmente restrittiva del criterio di giurisdizione, al giudizio *Bankovic* nel quale la Corte ha ritenuto che in assenza di controllo effettivo sul territorio estero, non rientrasse nella giurisdizione convenzionale il caso del civile ucciso da una bomba aerea sganciata da uno stato membro in territorio straniero. Cfr. Corte Europea dei Diritti dell'Uomo, Gran Camera, 19 dicembre 2001, ricorso no. 52207/99, *Decision as to the admissibility of application no. 52207/99 by Bankovic and Others v. Belgium and Others.*

[91] Così in *Al-Skeini*, dove la Corte ha ritenuto sussistente una responsabilità extraterritoriale del Regno Unito sulla base del controllo da esso esercitato sul territorio iracheno e l'uccisione, *ivi*, di diversi civili. Cfr. Corte Europea dei Diritti dell'Uomo, Gran Camera, 7 luglio 2011, ricorso no. 55721/07, *Case of Al-Skeini and Others V. The United Kingdom*. A conforto di quanto detto nel paragrafo si vedano anche C. MELONI, *Una importante pronuncia della Corte di Strasburgo in materia di tutela dei diritti umani nell'ambito di missioni militari all'estero. Riflessioni attorno alla sentenza della Corte EDU nel caso Al-Skeini c. Regno Unito del 7 luglio 2011*, in *Diritto Penale Contemporaneo*, 2011. M. MILANOVIC, *Surveillance and cyber operations*, in M. GIBNEY et al. (curr.), The Routledge Handbook of Extraterritorial Human Rights Obligations, 2022, 366-378.

[92] Si veda, ad esempio: *Merkel tells Obama: 'Spying on friends is unacceptable'*, in *BBC* (24 ottobre 2013), consultabile presso «https://www.bbc.com/news/av/world-europe-24659743». Ultimo accesso eseguito il 28.11. 2022.

irrisolta la questione se la più gran parte di esse siano anche solo ammesse a beneficiare della protezione CEDU. Soprattutto, l'approccio della Corte risulta tutt'altro che dirompente se comparato all'atteggiamento ben più avanguardista adottato l'anno precedente dalla corte costituzionale federale tedesca che, intervenendo proprio in tema di sorveglianza elettronica ed attestandosi su posizioni ben più ambiziose, ha espressamente sancito la vigenza, per il potere pubblico, del vincolo costituito dai diritti protetti dalla legge fondamentale anche laddove l'esercizio di tali poteri avvenga al difuori del territorio nazionale, pena la creazione di un'area di vuoto che farebbe indietreggiare la tutela dei diritti umani innanzi all'avanzare del progresso tecnologico e alla conseguente, crescente, porosità dei confini statali.[93] Non si può quindi che sperare che, sul solco di tale esempio virtuoso, la lacuna ad oggi esistente in ambito convenzionale venga colmata in futuro.

8. Conclusioni

Così esauriti i profili di studio oggetto delle sentenze e volendo da ciò trarre delle conclusioni di ordine generale quanto può dirsi è che con tali decisioni viene compiuto un passo importante nella disciplina delle intercettazioni di massa e nel loro adattamento allo spirito del tempo, attraverso l'identificazione di una serie di criteri/cautele più o meno rispettosi dell'accresciuta pervasività e portata dello strumento nel mondo contemporaneo. Che tale elaborazione costituisca il punto di arrivo della regolamentazione del fenomeno è, però, nella migliore delle ipotesi, discutibile, come appalesato dallo stesso, vivace, dibattito nato tra i giudici a margine delle sentenze, in cui opinione ricorrente è che si siano perse delle buone occasioni per fissare una disciplina del settore realmente garante dei diritti umani coinvolti.[94] Su tutte, una questione rimane aperta: dove fissare il punto di bilanciamento tra la tutela dei diritti umani lambiti dalle intercettazioni di massa e la necessità degli Stati di disporre di tale strumento per fronteggiare le nuove minacce alla propria sopravvivenza e a quella dei propri cittadini? Questione quantomai spinosa giacché attinente al contrasto tra interessi parimenti essenziali – e per molti versi esistenziali – della democrazia moderna.

Che i diritti umani alla vita privata e alla libertà di espressione/stampa siano suoi attributi essenziali è di agevole percezione: come argutamente messo in luce dagli stessi

[93] Per una trattazione più estesa della pronuncia tedesca e delle sue implicazioni si veda R. BIFULCO, *L'efficacia extraterritoriale dei diritti fondamentali in una storica sentenza del Tribunale costituzionale federale tedesco*, in *mediaLAWS: rivista di diritto dei media*, vol. 3, 2020, 283-297. Sul punto citato, in particolare, cfr. ibid. 291. Sugli esiti legislativi avuti in Germania dalla pronuncia si veda anche Katrin KAPPLER, *Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service: The Importance of Human Rights in the Cooperation of Intelligence Services*, in *German Law Journal*, vol. 23, n. 2, 173-185.

[94] Si veda, solo per fare un esempio, *Big Brother Watch*, n. 2 cit., *Joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak*, §30.

giudici, questi sono il presupposto per la fruizione di un'ampia schiera di diritti e libertà democratiche che solo al riparo dallo sguardo indiscreto del "grande fratello" – per usare l'allegoria Orwelliana – possono esercitarsi pienamente.[95] Infatti, se la gente sa o anche solo teme di essere spiata, difficilmente si opporrà ai detentori del potere facendo uso dei propri diritti di sciopero, manifestazione o anche solo di voto; pur se ritiene che questi sbaglino. Ancor meno potrà sfruttare i poteri di sanzione dell'operato del Governo messigli a disposizione dalla propria costituzione se non sa dei suoi abusi perché la stampa scomoda è stata sistematicamente intercettata e censurata. In tal contesto risulta chiaro come la sorveglianza di massa, nelle mani sbagliate, possa essere (ab)usata per coartare l'obbedienza e il conformismo e debba perciò essere attorniata di adeguate garanzie dei diritti umani minacciati.

Al contempo, un fantasma si aggira per l'Europa (e non solo) affliggendo i moderni Stati democratici: le quanto mai elusive minacce alla loro sopravvivenza, che in un mondo sempre più tecnologico e globalizzato sono anch'esse sempre più dematerializzate e quindi di forma intrinsecamente fluida. Di più, mentre una volta gli attentati alla sopravvivenza dello Stato erano prerogativa di altri attori statali o di compagini particolarmente ampie ed organizzate (come i gruppi insurrezionali), la dipendenza da internet delle moderne infrastrutture essenziali dà tale potere distruttivo anche al singolo, che a patto di avere una buona conoscenza del mezzo può, da solo, infliggergli enormi danni all'apparato statale (si pensi all'*hackeraggio* della rete elettrica nazionale o anche solo delle chiuse di una diga). Minacce, che quand'anche non giungessero a mettere a repentaglio l'esistenza dello Stato nel suo complesso potrebbero nondimeno attentare all'incolumità di un'ampia compagine di suoi cittadini e turbarne l'ordine pubblico, risultando peraltro particolarmente difficili da identificare e contrastare con gli strumenti tradizionali per via della loro matrice individuale, e quindi poco appariscente. Tali caratteri pongono evidentemente una domanda, a cui lo Stato, in quanto tutore dell'incolumità propria e dei propri cittadini, non può sottrarsi: come fronteggiare un nemico così sfuggente?

È chiaro che la prevenzione del fenomeno non può prescindere dall'uso degli stessi canali su cui questo si manifesta. Allo stesso modo, più sfuggente è la minaccia, più deve essere pervasivo il mezzo per fronteggiarla ma ciò implica che allora, questo, raggiungerà una platea necessariamente maggiore di soggetti, con ovvie ricadute sui loro diritti, primo tra tutti quello alla riservatezza. È questo l'intrinseco paradosso sotteso al tema delle intercettazioni di massa e che nelle decisioni della Corte trova espressione in varie soluzioni di compromesso più o meno efficaci, come nel caso eloquente delle attività di sviluppo svedesi: necessarie all'adeguamento tecnico del Paese rispetto all'evolversi delle minacce esterne e come tali ammesse ma nondimeno costituenti un'ipotesi eccentrica (e sfuggente) rispetto alla rigida elencazione fatta dal

[95] Ibid. §§3-8.

legislatore di casi giustificanti le intercettazioni di massa. Ma gli esempi, come si è visto, sono molteplici.

Tale contributo ha cercato di esporre in modo quanto più analitico tali importanti decisioni, le loro ragioni ispiratrici, i loro meriti e le corrispondenti problematiche. Se il punto di equilibrio trovato dalla CEDU in tutte queste ipotesi sia meritevole di condivisione o richieda ulteriore *labor limae* è una valutazione che ora si lascia alla sensibilità del lettore, alla luce delle considerazioni esposte, della dottrina riportata e delle intrinseche tensioni tra contrapposti interessi che pervadono la materia e la aprono ad opinioni differenti; nella consapevolezza che l'attualità delle intercettazioni di massa renda le sentenze esaminate solo le prime puntate di una più ampia saga che non mancherà di fornire agli operatori del diritto interessanti spunti di riflessione. È infatti notizia recente che diversi Stati europei avrebbero fatto ricorso al sistema *Pegasus*, in grado di condurre intercettazioni mirate di un ampissimo numero di telefoni cellulari.[96] Non rimane dunque che attendere, dovendosi, per contro, arrestare qui la presente analisi.

[96] Così F. DUBUISSON, n. 79 cit., 141; AMNESTY INTERNATIONAL, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, 23 luglio 2021. Consultabile presso: «https://www.amnesty.org/en/documents/doc10/4491/2021/en/», ultimo accesso eseguito il 28.11.2022.