NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

# *La normalizzazione della sorveglianza di massa nel contesto della CEDU e il Quarto Oxford Statement sulle tutele offerte dal diritto internazionale nel cyberspazio**

**di Flavia Zorzi Giustiniani****

Nel periodo qui in rassegna devono segnalarsi anzitutto due pronunce, relative alle operazioni di sorveglianza elettronica di massa, che sono state emesse il 25 maggio scorso dalla Grande Camera della Corte europea dei diritti dell'uomo.

La prima sentenza è stata resa nel **caso *Big Brother Watch & Altri c. Regno Unito***[1]. La decisione giunge al termine di un lungo *iter* processuale, iniziato nel 2013 da 16 organizzazioni e giornalisti attivi nel campo della tutela dei diritti civili e della libertà di stampa a seguito delle rivelazioni di Edward Snowden che dettero avvio al c.d. *Datagate*. I ricorrenti ritenevano che determinati sistemi di sorveglianza generalizzata delle comunicazioni elettroniche, utilizzati dal Regno Unito nell'ambito di attività d'*intelligence* per ragioni di sicurezza nazionale, violassero gli articoli 8 e 10 della CEDU[2].

La sentenza resa il 13 settembre del 2018 dalla Prima Sezione della Corte, pur riconoscendo che alcuni aspetti del regime di sorveglianza britannico, all'epoca dei fatti disciplinato dal *Regulation of Investigatory Powers Act* (RIPA) del 2000[3], violassero gli articoli 8 e 10 della Convenzione a motivo di insufficienti garanzie procedurali, non aveva considerato di per sé inammissibile l'intercettazione di massa. In particolare, la Camera aveva ritenuto che i governi nazionali godono di un ampio margine di apprezzamento nel decidere quali misure sono necessarie per garantire la sicurezza nazionale[4] e che l'autorizzazione giudiziaria al fine di operare intercettazioni di massa è soltanto "altamente auspicabile" e non indispensabile per garantire il rispetto dell'art. 8 della Convenzione[5]. Nella richiesta di rinvio alla Grande Camera i ricorrenti lamentavano, tra l'altro, il riconoscimento poco argomentato effettuato dalla Prima Sezione della proporzionalità di sistemi di sorveglianza generalizzata.

Nella sua decisione la Grande Camera ha sostenuto che un regime di sorveglianza di massa di per sé non è contrario alla Convenzione e ne ha confermato la legittimità dinanzi alle numerose

---

*Contributo sottoposto a *peer review*.

** Professoressa associata di diritto dell'Unione europea, Link Campus University

[1] Corte europea dei diritti dell'uomo, ricorsi n. 58170/13, 62322/14 et 24960/15.

[2] In particolare l'intercettazione di massa delle comunicazioni; la ricezione di materiale di intercettazione da governi stranieri e agenzie di intelligence; nonché l'ottenimento di dati di comunicazione dai fornitori di servizi di comunicazione.

[3] Il RIPA é stato poi sostituito dall'*Investigatory Powers Act* nel 2016.

[4] Cfr. *Big Brother Watch & Altri c. Regno Unito*, Prima Sezione, sentenza del 13 settembre 2018, par. 314-315, 387.

[5] *Ibid.*, par. 381.



ISSN 2279-7238

minacce alle quali sono esposti gli Stati nell'epoca attuale[6]. La Grande Camera ha ribadito quanto già affermato dalla Prima Sezione, ovvero che le autorità nazionali godono di un ampio margine di apprezzamento nello scegliere come meglio proteggere la sicurezza nazionale[7]. Il suddetto regime di sorveglianza, tuttavia, deve essere soggetto ad un controllo "end-to-end" al fine di minimizzare il rischio di abusi. Nella specie ciò significa, secondo la Corte, che a livello nazionale dovrebbe essere fatta una valutazione della necessità e della proporzionalità delle misure adottate in ogni fase del processo; che l'intercettazione di massa dovrebbe essere soggetta ad un'autorizzazione indipendente all'inizio, quando l'oggetto e la portata dell'operazione sono stati definiti; e che l'operazione dovrebbe essere soggetta alla supervisione e ad un esame indipendente *ex post*[8]. Con riguardo al regime di intercettazione britannico la Grande Camera ha poi riscontrato tre carenze fondamentali: che l'intercettazione di massa non è stata autorizzata da un organismo indipendente dall'esecutivo (bensì dal Segretario di Stato); che non sono state specificate categorie di termini di ricerca che definiscano le tipologie di comunicazioni da esaminare; e infine, che non era stato autorizzato l'uso di identificatori specifici (legati ad un singolo individuo)[9].

I giudici hanno quindi ritenuto che il regime di intercettazioni di massa contenuto nella sezione 8(4) del RIPA non soddisfaceva il requisito di "qualità del diritto", violando così l'articolo 8 della CEDU[10]. La Grande Camera ha poi stabilito, allineandosi a quanto deciso dalla Prima Sezione, che l'intercettazione di massa delle comunicazioni come l'acquisizione di dati dai fornitori di servizi di comunicazione hanno violato l'art. 10, in quanto sprovviste di garanzie relativamente alle fonti giornalistiche e al materiale giornalistico riservato[11].

Quanto al sistema di condivisione di dati attraverso il quale il Regno Unito riceveva materiale dai servizi di *intelligence* statunitensi, la maggioranza dei giudici non l'ha considerato contrario agli articoli 8 e 10 della Convenzione[12]. Secondo il collegio, infatti, tale condivisione di informazioni è ammissibile a patto che siano previste garanzie adeguate contro gli abusi e che il regime sia soggetto ad un controllo indipendente e ad un riesame *ex post*[13]. I cinque giudici dissenzienti hanno invece lamentato l'assenza dei necessari meccanismi per controllare il potenziale uso improprio dei poteri di sorveglianza[14].

Va rilevato che la Grande Camera si è soffermata soltanto sulle garanzie relative alla ricezione di dati da parte di autorità estere, ivi comprese le norme per la richiesta e la ricezione di *intelligence* e le garanzie per l'esame, l'uso, l'archiviazione, la trasmissione, la cancellazione e la distruzione del materiale ricevuto esistenti nel Regno Unito. Non ha invece considerato il caso, inverso, in cui sia uno Stato parte della CEDU (nella specie il Regno Unito) ad inviare informazioni ad uno Stato terzo (nella specie gli USA), e l'eventuale applicazione extraterritoriale della Convenzione che ciò implicherebbe. In tale scenario, come è stato osservato, se l'attenzione della Corte fosse concentrata solo sulle garanzie interne e non su quelle esistenti nel Paese con cui sono condivisi

[6] Nelle parole della Corte, l'intercettazione di massa di comunicazioni straniere costituisce "a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime" (*Big Brother Watch & Altri c. Regno Unito*, Grande Camera, sentenza del 25 maggio 2021, par. 386).
[7] *Ibid.*, par. 228.
[8] *Ibid.*, par. 350.
[9] *Ibid.*, par. 425.
[10] *Ibid.*, par. 426.
[11] *Ibid.*, par. 456-458, 524-528.
[12] *Ibid.*, par. 510-514, 515-516.
[13] *Ibid.*, par. 350.
[14] Cfr. Opinione parzialmente dissidente dei giudici Lemmens, Vehabović, Ranzoni and Bošnjak, par. 3 ss.; Opinione parzialmente concorrente e parzialmente dissidente del giudice Pinto de Albuquerque, par. IV.B.

i dati, i residenti britannici potrebbe trovarsi esposti ad un uso improprio dei loro dati personali da parte delle autorità straniere[15].

Quanto alle garanzie che dovrebbero essere fornite dal diritto interno per rendere ammissibile un sistema di monitoraggio di massa, la Grande Camera ha prospettato una serie di criteri più ampia rispetto a quanto già indicato in precedenza nel caso *Weber*[16]. Al fine di assicurare che il regime di intercettazioni di massa non si risolva in una violazione dell'art. 8, il diritto nazionale dovrebbe definire: 1) i motivi per i quali l'intercettazione di massa può essere autorizzata; 2) le circostanze in cui le comunicazioni di un individuo possono essere intercettate; 3) la procedura da seguire per il rilascio dell'autorizzazione; 4) le procedure da seguire per la selezione, l'esame e l'utilizzo del materiale di intercettazione; 5) le precauzioni da prendere nella comunicazione del materiale ad altri soggetti; 6) i limiti alla durata dell'intercettazione, alla conservazione del materiale intercettato e alle circostanze in cui tale materiale deve essere cancellato e distrutto; 7) le procedure e le modalità per il controllo da parte di un'autorità indipendente del rispetto delle suddette garanzie e dei suoi poteri per far fronte alle inadempienze; 8) le procedure per l'esame indipendente ex post di tale conformità e i poteri conferiti all'organo competente nel far fronte ai casi di non conformità[17].

Dopo aver confermato la legittimità *prima facie* della sorveglianza di massa, la Corte si è quindi focalizzata esclusivamente sulle garanzie procedurali, dimostrando quello che è stato definito una sorta di "feticismo procedurale"[18]. Peraltro, dopo aver fatto riferimento ai suddetti otto criteri sulla cui base valutare la normativa interna sulle intercettazioni di massa, la Grande Camera ha aggiunto che tali criteri fanno parte di una "valutazione globale" della proporzionalità del programma[19]. Non è dunque chiaro se gli stessi debbano essere rispettati integralmente o meno.

La sentenza della Grande Camera è stata accolta come un "important win for privacy and freedom for everyone in the UK and beyond"[20]. A ben vedere, tuttavia, la decisione si segnala al contrario per aver sancito che la sorveglianza di massa in linea di principio non è né illegale né sproporzionata[21]. Solo uno dei 17 giudici, Pinto de Albuquerque, nella sua opinione separata si è opposto nettamente alla pratica della sorveglianza di massa, rimarcando che "l'utilità [delle intercettazioni] non è la stessa cosa della necessità e della proporzionalità in una società

---

[15] Cfr. M. Zainieriute, "Procedural Fetishism and Mass Surveillance under the ECHR Big Brother Watch v. UK", 2 giugno 2021, disponibile al link https://verfassungsblog.de/big-b-v-uk/.

[16] Cfr. Corte europea dei diritti dell'uomo, *Weber e Saravia c. Germania*, ricorso n. 54934/00, decisione del 29 giugno 2006. I sei criteri enunciati in questa sentenza erano stati originariamente dettati per le intercettazioni mirate.

[17] Cfr. *Big Brother Watch & Altri* cit., par. 361.

[18] Cfr. M. Zainieriute, cit.

[19] Cfr. *Big Brother Watch & Altri* cit., par. 360.

[20] *Sic* Privacy International (cfr. "Human rights groups win European Court of Human Rights claim on UK mass surveillance regime", disponibile al link https://www.privacyinternational.org/press-release/4522/human-rights-groups-win-european-court-human-rights-claim-uk-mass-surveillance).

[21] V. tra gli altri : E. Watt, "Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK", 28 giugno 2021, disponibile al link https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/; J. Sajfert, "The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?", 8 giugno 2021, in European Law Blog, disponibile al link https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/.

democratica"[22] e censurando poi la sentenza per aver aperto le porte ad un Grande Fratello elettronico in Europa[23].

La seconda sentenza, anch'essa emessa dalla Corte nella sua massima composizione e nella stessa data, concerne il caso *Centrum för Rättvisa c. Svezia.* All'origine vi é un ricorso presentato nel 2008 dalla ONG *Centrum för Rättvisa*, secondo la quale la legge svedese sulla *signals intelligence*[24] violava la privacy ai sensi dell'art. 8 CEDU. Il 19 giugno 2018 la Terza Sezione della Corte aveva stabilito, all'unanimità, che il sistema di intercettazione massiccia svedese non era contrario alla Convenzione. La Grande Camera ha accolto invece le doglianze dei ricorrenti riscontrando la violazione dell'art. 8 da parte della legislazione svedese per: l'assenza di regole chiare sulla distruzione del materiale intercettato, laddove non contenga dati personali[25]; la possibilità di trasmettere il materiale intercettato a Stati terzi senza tenere in considerazione la *privacy* degli individui interessati[26]; nonché l'assenza di un effettivo meccanismo di controllo *ex post facto* sullo svolgimento delle operazioni[27]. Anche in questo caso, tuttavia, la Grande Camera ha messo in evidenza che le intercettazioni di massa sono di importanza vitale per le Parti Contraenti al fine di identificare minacce alla loro sicurezza e che nessuna alternativa o combinazione di alternative sarebbe idonea a sostituire il potere di effettuare intercettazioni di massa[28].

Il fatto che la legislazione svedese sia stata censurata dalla Corte in misura assai minore rispetto a quella britannica nel caso *Big Brother Watch* non significa necessariamente che la prima ponga meno problemi sul fronte del rispetto dei diritti fondamentali. Secondo il giudice dissidente Pinto de Albuquerque la maggioranza pare assumere la veridicità di quanto sostenuto dal governo svedese nelle sue memorie senza compiere una reale verifica[29]. Come è stato osservato in dottrina, peraltro, malgrado la legislazione svedese sia "highly opaque", i giudici non hanno analizzato in alcun modo né la giurisprudenza della *Swedish Foreign Intelligence Court* né la prassi della *Försvarets radioanstalt* (l'autorità nazionale per la *signals intelligence*)[30].

In generale, l'effetto delle due sentenze qui in rassegna sarà probabilmente quello di condurre, come paventato da più parti, ad una "normalizzazione" della sorveglianza di massa nei decenni a venire[31].

Un'altra novità degna di nota è poi la pubblicazione, avvenuta il 2 giugno scorso, dell'*Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities*[32]. Si tratta del quarto *statement* realizzato nell'ambito dell'*Oxford Process on International Law Protections in Cyberspace*, lanciato nel maggio 2020 dall'*Oxford Institute for Ethics, Law and Armed*

---

[22] Cfr. Opinione parzialmente concorrente e parzialmente dissidente cit., par. 58.

[23] *Ibid.*, par. 59-60. I giudici Lemmens, Vehabović e Bošnjak, pur concordando parzialmente, hanno affermato l'esigenza di maggiori garanzie.

[24] La *signals intelligence* consiste nella raccolta, combinazione e analisi di segnali, sia questi emessi da persone che da macchinari.

[25] Cfr. *Centrum för Rättvisa c. Svezia*, sentenza del 25 maggio 2021, Grande Camera, par. 342.

[26] *Ibid.*, par. 326-330.

[27] *Ibid.*, par. 359-364.

[28] *Ibid.*, par. 365.

[29] Cfr. Opinione parzialmente concorrente e parzialmente dissidente cit., sez. B.

[30] Cfr. M. Klamberg, "Big Brother's Little, More Dangerous Brother. Centrum för Rättvisa v. Sweden", in Verfassungsblog on Matters Constitutional, disponibile al link https://verfassungsblog.de/raettvisa/.

[31] *Sic.* M. Milanovic, "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa", in EJIL: Talk! Blog of the European Journal of International Law, 26 maggio 2021, disponibile al link https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

[32] Cfr. https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities#/.

*Conflict* con l'intento di identificare le norme di diritto internazionale che sono applicabili al cyberspazio e chiarirne la portata in una serie di contesti sensibili. Più in particolare gli *Oxford Statements* enucleano brevemente le regole che disciplinano le operazioni cibernetiche dirette a specifici oggetti protetti e sulle quali si registra un livello di consenso adeguato sul piano internazionale[33].

Il quarto *Statement* delinea una serie di obblighi degli Stati, sia positivi che negativi, con riguardo a "information operations and activities" quali *inter alia* la disinformazione, i discorsi d'odio ed altri discorsi che, potendo raggiungere istantaneamente una vastissima platea di destinatari, hanno la capacità di causare danni fisici o non fisici a singoli, Stati ed entità private. Tali obblighi, che devono trovare applicazione sia nelle condotte statali interne che internazionali, si fondano su alcuni principi e normative chiave del diritto internazionale, segnatamente la sovranità, il non intervento, il diritto internazionale dei diritti umani e il diritto internazionale umanitario.

Nella parte preambolare dello *Statement* si ricorda tra l'altro che anche le società, come descritto nei Principi 11 e 12 dei Principi guida delle Nazioni Unite su imprese e diritti umani[34], hanno la responsabilità di rispettare i diritti umani degli individui e che tale responsabilità si estende all'impatto delle operazioni e attività informative condotte mediante l'uso dei loro servizi. Quanto agli obblighi degli Stati, lo Statement afferma *inter alia* i seguenti obblighi negativi: astenersi dall'intraprendere, sostenere o consentire nell'ambito della loro giurisdizione forme di discorso che sono vietate dal diritto internazionale, come qualunque propaganda di guerra e qualsiasi difesa dell'odio nazionale, razziale o religioso che costituisca incitamento alla discriminazione, all'ostilità o alla violenza[35]; astenersi dall'intraprendere o supportare qualsiasi altra operazione o attività informativa che violi i diritti degli individui all'interno della loro giurisdizione, come il diritto alla vita, alla salute, alla vita privata, alla libertà di pensiero e di opinione, alla libertà di espressione, ivi compresa la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, il diritto di votare e partecipare alla cosa pubblica[36]. Il primo obbligo è accompagnato poi da un obbligo, stavolta positivo, di proibire per legge operazioni e attività informative assimilabili alle forme di discorso menzionate[37].

Ad oggi lo *Statement* è stato sottoscritto da più di 110 giuristi di fama internazionale[38].

---

[33] Del terzo *Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means* si era dato conto nella rassegna intitolata "Governing the ungoverned. Recenti proposte europee e internazionali per regolare il digitale", apparsa sul n. 3/2020 di questa Rivista (e disponibile al link https://www.nomos-leattualitaneldiritto.it/nomos/flavia-zorzi-giustiniani-governing-the-ungoverned-recenti-proposte-europee-e-internazionali-per-regolare-il-digitale/).

[34] ONU, Guiding Principles on Business and Human Rights: *Implementing the United Nations "Protect, Respect and Remedy" framework*, 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[35] Cfr. il principio 3.

[36] Cfr. il principio 4.

[37] Cfr. il principio 3.

[38] L'elenco é disponibile al seguente link: https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities#/.