Classificazione

Art. 8 CEDU – Diritto al rispetto della vita privata e familiare – Art. 10 CEDU – Libertà di espressione – **Intercettazioni di massa di comunicazioni o conversazioni** – Inquadramento giuridico delle forme di *Intelligence* elettromagnetica (ROEM) – Minacce poste agli Stati dalle reti internazionali che utilizzano Internet per comunicare – Conformità convenzionale – Condizioni.

Riferimenti normativi convenzionali

CEDU, art. 8, 10, 41.

Riferimenti normativi per l'ordinamento italiano

Cost., artt. 3, 15; artt. 266, 267 cod. proc. pen.; art. 132, d.lgs. 30 giugno 2003, n. 196

Riferimenti giurisprudenziali

Sentenze della Corte EDU

Breyer c. Germania, 30 gennaio 2020, n. 50001/12; Zakharov c. Russia, 4 dicembre 2015, n. 47143/06; Liberty e altri c. Regno Unito, 1/7/2008; Weber e Saravia c. Germania, dec. n. 54934/00 del 29/6/2006; Pantano c. Italia, 6 novembre 2003, n. 60851/00; Huvig c. Francia, 24 aprile 1990; Kruslin c. Francia, 24/4/1990.

Sentenze della Corte di Giustizia dell'Unione Europea

Grande Sez., 2 marzo 2021, C-746/18, U.K. c. Prokuratuur; Grande Sez., 6 ottobre 2020, La Quadrature du net e aa. (C-511/18, C-512/18, C-520/18); Grande Sez., 6 ottobre 2020, Privacy International (C-623/17); Grande Sez., 2 ottobre 2018, Ministerio Fiscal (C-207/16); Grande Sez., 21 dicembre 2016, Tele 2 Swerige AB e a. (C-203/15 e C-698/15); Grande Sez., 8 aprile 2014, Digital Rights Ireland Ldt e a. (C-293/12 e C-594/12).

Sentenza della Corte di cassazione

Sez. 2, n. 5741 del 10/12/2019, Dedej, Rv. 278568-01; Sez. 3, n. 48737 del 25/09/2019, R., Rv. 277353-01; Sez. 5, n. 33851 del 24/04/2018, M., Rv. 273892-01.

Pronunce segnalate

Corte EDU, Centrum för rättvisa c. Svezia, 25 maggio 2021, ricorso n. 164/2021.

Corte EDU, Grande Camera, Big Brothers Watch e altri c. Regno Unito, 25 maggio 2021, ricorsi n. 58170/13, 62322/14 e 24960/15.

Abstract

La Corte Edu, Grande Camera, ha ritenuto sussistente la violazione degli artt. 8 e 10 della Convenzione in relazione ad ***un sistema di intercettazioni di massa concernente sia il contenuto delle conversazioni che i dati ad esse relativi****,* ***allorché la legislazione nazionale non preveda****: a) la necessità di un'****autorizzazione*** *preventiva di tali intercettazioni da parte di un* ***giudice o di un organo indipendente dall'esecutivo****; b) la possibilità di un* ***controllo successivo*** *da parte di un organo parimenti indipendente, non necessariamente giudiziario, dei dati acquisiti, soprattutto in caso di acquisizioni "accidentali" di dati concernenti le comunicazioni dei giornalisti; c) le parole chiave in base alle quali le comunicazioni intercettate verranno poi selezionate ed esaminate.*

I) Il caso Centrum för rättvisa c. Svezia

Con la pronuncia in esame la Corte EDU si pronunciava sul ricorso proposto dal "Centrum för rättvisa", una fondazione senza scopo di lucro che ha sede a Stoccolma, costituita nel 2002; essa rappresenta i suoi assistiti nelle controversie sui diritti, soprattutto nei confronti dello Stato.

La parte ricorrente, in particolare, prospettava il rischio che le sue comunicazioni fossero state intercettate per mezzo di strumenti di intelligence elettromagnetica, che avevano consentito la captazione sistematica delle comunicazioni su base giornaliera tra soggetti privati, organizzazioni e aziende, svedesi ed estere, tramite e-mail, telefono e fax. Tali forme di intercettazione erano intervenute per ragioni di sicurezza, interna ed estera, senza che fossero preventivamente chiari i presupposti e i limiti entro cui i dati telematici potevano essere acquisiti e conservati presso appositi archivi informatici.

Occorre precisare ulteriormente che la parte ricorrente non aveva avviato alcun procedimento interno, sostenendo che non vi era rimedio effettivo per le sue denunce alla Convenzione.

Il ricorso, pertanto, pone il problema dell'inquadramento delle forme di intelligence elettromagnetica, definite con l'acronimo di **ROEM,** che viene definita dalla Corte EDU come **l'attività finalizzata a intercettare, elaborare, analizzare e**

riportare informazioni trasmesse da segnali elettronici, che possono essere convertiti in testo, immagine o suono.

La risoluzione di tale questione ermeneutica veniva affrontata dalla Corte EDU sulla base di un'accurata ricognizione del sistema normativo svedese, nel quale la raccolta di segnali elettronici convertibili è una forma di intelligence disciplinata dalle leggi interne, cha ne attribuiscono il controllo istituzionale all'Istituto Nazionale di Difesa Radio, che è un'agenzia governativa operante sotto la vigilanza del Ministero della Difesa, autorizzata allo svolgimento di forme di intelligence elettromagnetica, realizzate attraverso strumenti di intercettazione di massa.

Tale Istituto è composto da un giudice e da altri membri nominati per un quadriennio e svolge la sua attività in assoluta segretezza.

La decisione della Corte EDU

La Corte EDU accoglieva il ricorso proposto dal "Centrum för rättvisa", ritenendo, che, sulla base della prospettazione della parte ricorrente, doveva ritenersi violata la norma dell'art. 8, par. 2, CEDU, a tenore del quale non può esservi ingerenza di un'autorità pubblica nell'esercizio del diritto alla riservatezza «a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

L'assunto ermeneutico da cui muoveva la Corte EDU traeva origine dalla constatazione della proliferazione delle minacce poste agli Stati membri dagli utenti della rete telematica, pubblici e privati: esse comportano il pericolo di intercettazioni illegali realizzate attraverso sofisticate tecnologie, fermo restando che l'uso di forme preventive di massa, in quanto tali, soprattutto laddove effettuate per ragioni di sicurezza, non può essere ritenuto contrario alla disposizione dell'art. 8 CEDU.

In questa cornice, la Corte EDU riteneva che, in considerazione del costante sviluppo delle tecnologie comunicative, le forme di intercettazione di massa comportano il rischio potenziali di abusi telematici seriali, idonei a determinare la lesione dei diritti individuali delle persone e degli enti giuridici; ne deriva la necessità di bilanciare le esigenze di sicurezza collettiva – a garanzia delle quali viene ribadita la legittimità di forme di intercettazione di massa, realizzata con meccanismi di intelligence elettromagnetica – con le prerogative di libertà

individuale, mediante un giudizio che deve essere eseguito, caso per caso, sulla base della preliminare ricognizione dei sistemi giuridici di riferimento.

Occorre, pertanto, valutare in concreto la **proporzionalità** delle misure adottate per assicurare la realizzazione di forme di intelligence elettromagnetica rispettose dell'art. 4, che postulano una verifica sulla legittimità di ogni fase del percorso applicativo degli strumenti di intercettazione di massa; le relative operazioni devono essere sottoposte a un controllo adeguato, eseguito da autorità indipendenti, sia all'inizio sia alla fine di ciascun segmento del procedimento captativo, sul modello dell'Istituto Nazionale di Difesa Radio, che, sul piano dei principi, appare idoneo a soddisfare le esigenze che si sono richiamate.

Tuttavia, tale verifica, secondo la Corte EDU, deve essere eseguita nel rispetto di alcuni parametri essenziali, che devono essere definiti dal diritto nazionale in modo che il regime in questione possa essere considerato conforme ai principi della Convenzione EDU e dare luogo al bilanciamento delle esigenze che si sono richiamate nel rispetto della giurisprudenza convenzionale (Breyer c. Germania, 30 gennaio 2020, n. 50001/12).

Applicando questi parametri ermeneutici al regime svedese di intercettazione di massa, la Corte EDU rilevava che i servizi di *intelligence* del Paese scandinavo hanno compiuto un grande sforzo di contemperare le esigenze di sicurezza e individuale richiamate, pur essendosi create talune disarmonie applicative che meritavano di essere segnalate.

Tali disarmonie applicative, che imponevano una rimeditazione complessiva del sistema di intercettazione di massa svedese, in particolare, riguardavano 1) l'assenza di una norma chiara in materia di distruzione dei dati intercettati, laddove non contenenti dati personali; 2) il fatto che la legge svedese non precisava quali fossero i meccanismi di tutela dei diritti individuali quando le informazioni acquisite venivano condivise con *partners* stranieri; 3) quali erano i parametri applicabili per massimizzare le forme di controllo *a posteriori* delle informazioni acquisite.

II) Il caso Big Brother Watch e altri c. Regno Unito

Con tre separati ricorsi, le organizzazioni impegnate nella promozione delle libertà civili e dei diritti dei giornalisti e i singoli soggetti (tutti indicati nell'elenco allegato alla sentenza in commento) hanno dedotto che, a causa delle loro attività, era probabile che le loro comunicazioni elettroniche di carattere trans-nazionale fossero state intercettate dal servizio segreto del Regno Unito o da questo ricevute da altri governi stranieri o, infine, ottenute dal Regno Unito dai fornitori dei relativi servizi.

Al momento della domanda il regime delle intercettazioni di massa era disciplinato all'interno del sistema britannico dal c.d. **RIPA** (Regulation of Investigatory Powers Act) del 2000 e consentiva al Segretario di Stato di autorizzare, nell'interesse della sicurezza nazionale, un mandato relativo a tali intercettazioni – concernenti le comunicazioni "esterne" in quanto inviate o ricevute al di fuori del territorio del Regno Unito, a condizione che fossero necessarie per prevenire o investigare su gravi reati, o per la salvaguardia del benessere economico del Regno Unito, e proporzionate allo scopo perseguito.
Inoltre, in base ad un accordo del 5 marzo 1946 tra Regno Unito e Stati Uniti di America, è consentito lo scambio tra i due Paesi delle informazioni relative a tali comunicazioni "esterne".

La decisione della Corte EDU

a) Le garanzie necessarie nel sistema di intercettazioni di massa

La Corte ha accolto parzialmente i ricorsi sulla base di considerazioni analoghe a quelle esaminate nel caso che precede.
Tenuto conto della legislazione internazionale in materia (in particolare, la Risoluzione dell'Assemblea Generale delle Nazioni Unite n. 68/167 del 18/12/2013 e la Convenzione del Consiglio di Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 28 gennaio 1981), del diritto dell'Unione (artt. 7, 8 e 11 della Carta di Nizza e le Direttive sulla protezione dei dati personali) nonché della giurisprudenza della Corte di Giustizia dell'Unione Europea in materia, la Corte EDU ha affermato che, **in linea generale, l'art. 8 della Convenzione non vieta l'uso del sistema delle intercettazioni di massa** (ad oggi ammesso da Finlandia, Francia, Germania, Olanda, Svezia, Svizzera e Regno Unito) **per proteggere la sicurezza nazionale o altri interessi nazionali contro serie minacce esterne.** A tal riguardo, precisa la Corte, gli Stati godono di un ampio margine di discrezionalità nel decidere quale sistema di intercettazione adottare a tale scopo, ma tale margine di discrezionalità va poi a restringersi nella fase operativa in cui è necessaria l'adozione di numerose garanzie a tutela da forme di arbitrio e di abuso.
Nel procedere alla valutazione della qualità della "base legale" legittimante un siffatto sistema, la Corte, ribadendo precedenti arresti in tema di intercettazioni (tra le altre, con particolare riferimento alle intercettazioni di massa, Corte EDU, Weber e Saravia c. Germania, dec. n. 54934/00 del 29/6/2006), ha individuato, oltre ai requisiti della **accessibilità e prevedibilità**, sei garanzie minime (**c.d. garanzie "Weber")** che la legge dovrebbe prevedere per evitare detti abusi in materia di

intercettazioni: 1) **la natura dei reati** che possono giustificare un provvedimento di intercettazione; 2) **la predeterminazione dei soggetti che possono essere intercettati;** 3) il **limite di durata** delle intercettazioni; 4) **la procedura da seguire** per esaminare, utilizzare e conservare i dati ottenuti; 5) **le precauzioni da adottare quando tali dati vengono comunicati a terzi;** 6) le circostanze in presenza delle quali i dati intercettati devono essere **cancellati o distrutti**.

Tali garanzie minime, precisa la Corte, rilevano non solo con riferimento alle intercettazioni del contenuto delle comunicazioni, ma anche nel caso, come quello in esame, in cui sia consentita anche l'acquisizione di massa dei dati relativi a dette comunicazioni, in quanto idonee a rivelare informazioni sulla vita privata, come l'identità o la posizione geografica di chi invia o riceve la comunicazione.

Tenuto conto della **natura "preventiva" delle intercettazioni di massa rispetto a quelle con destinatario predeterminato**, la Corte ha rilevato che le prime due garanzie, tra le sei sopra specificate, non sono direttamente applicabili al sistema delle intercettazioni di massa. Tuttavia, ha ritenuto indispensabile che, allorché uno Stato decida di adottare tale sistema, la legge contenga delle norme dettagliate sulle condizioni in presenza delle quali le autorità possono ricorrere a tali misure.

Ciò premesso, la Corte ha rilevato che il sistema delle intercettazioni di massa si sviluppa in **quattro diverse fasi** cui consegue una crescente interferenza nella vita privata.

Nella prima fase si procede alle intercettazioni di massa delle comunicazioni e dei dati ad esse relativi.

Nella fase successiva si procede alla individuazione delle comunicazioni di possibile interesse investigativo – e, dunque, anche dei soggetti che ne sono protagonisti – sulla base di parole chiave, "selettori", che possono anche avere una connotazione particolarmente "forte" (come, ad esempio, ove si utilizzi l'indirizzo di posta elettronica di un determinato soggetto per selezionare il materiale intercettato).

Le fasi successive attengono, infine, all'analisi ad opera di specialisti del contenuto delle comunicazioni selezionate ed al loro utilizzo, divulgazione o trasmissione a servizi segreti stranieri.

Al fine di ridurre al minimo il rischio di abusi di potere e di assicurare **che ogni interferenza risponda al requisito della "necessità in una società democratica**", la Corte ha affermato che l'intero processo deve essere soggetto ad un costante controllo, dal principio alla fine ("*end to ed safeguards*"), in merito alla necessità e proporzionalità delle misure adottate. Ciò comporta che ogni fase del processo relativo alle intercettazioni di massa – inclusa **l'autorizzazione iniziale**, l'individuazione dei "selettori" delle comunicazioni, l'utilizzo, conservazione e

distruzione delle stesse – deve essere oggetto di controllo **da parte di un giudice o, comunque, di un organo terzo, indipendente dall'esecutivo.**

Tale controllo dovrà essere assicurato **anche *ex post***. Infatti, chiunque sospetti che le proprie comunicazioni siano intercettate dai servizi segreti deve poter accedere ad un rimedio effettivo attraverso **la possibilità di un ricorso** dinanzi ad un organo indipendente, non necessariamente giudiziario, le cui decisioni dovranno essere legalmente vincolanti.

Analogamente garanzie dovranno essere assicurate anche nella condivisione con i servizi segreti di altri Stati (anche non contraenti) del materiale così intercettato. Tale condivisione potrà riguardare solo il materiale ottenuto attraverso un sistema conforme alla Convenzione e dovrà rispettare le seguenti ulteriori garanzie: 1) fondamento legale dello scambio, con la specifica previsione delle circostanze in presenza delle quali è possibile tale condivisione; 2) lo Stato "trasferente" dovrà assicurarsi che lo Stato ricevente abbia adottato misure idonee a prevenire abusi; 3) adozione di garanzie maggiori quando si tratta di informazioni "confidenziali", ad esempio relative all'attività dei giornalisti; 4) necessità che il trasferimento sia sottoposto ad un controllo da parte di un organo indipendente.

Analoghe garanzie, sia pure attraverso previsioni legali che non siano necessariamente identiche a quelle adottate per le intercettazioni, dovranno essere assicurate anche nell'ipotesi di acquisizione di massa dei dati relativi alle comunicazioni che, ad avviso della Corte EDU, non possono considerarsi di per sé meno intrusive dell'intercettazione del relativo contenuto.

b) La decisione del caso concreto

Con riferimento al caso concreto, la Corte ha ravvisato una violazione dell'art. 8 della Convenzione rilevando che la disciplina britannica non contiene sufficienti garanzie idonee a prevenire il rischio di abusi dall'inizio alla fine del procedimento avuto riguardo, tra l'altro ai seguenti fattori: mancanza di una previsione relativa all'iniziale autorizzazione da parte di un organo indipendente; mancata preventiva identificazione dei "selettori" delle comunicazioni; mancanza di prevedibilità delle circostanze in cui le comunicazioni possono essere esaminate.

Sulla base di analoghe considerazioni la Corte ha ravvisato, inoltre, una violazione dell'art. 10 della Convenzione. Pur distinguendo tra intercettazioni dirette e intercettazioni accidentali, la Corte ha rilevato che l'uso dei selettori, siano essi generici o di carattere "forte" (in quanto, ad esempio, correlati all'attività di un giornalista ed idonei a selezionare materiale confidenziale o ad individuarne le fonti), deve, comunque, essere soggetto ad un controllo da parte di un giudice o di

un organo indipendente, di carattere preventivo ovvero, in caso di intercettazioni accidentali, di carattere successivo (quest'ultima in relazione all'analisi, uso, conservazione, trasmissione e distruzione del relativo materiale).
Quanto allo scambio di informazioni con i servizi segreti americani, la Corte ha ritenuto che, alla luce delle garanzie adottate, non vi sia stata, invece, alcuna violazione degli artt. 8 e 10 della Convenzione.
Infine, quanto al regime di acquisizione diretta dei dati presso i fornitori dei servizi, la Corte ha ravvisato una violazione degli artt. 8 e 10 della Convenzione rilevando che un siffatto regime dovrebbe essere circoscritto alla lotta contro crimini gravi *("serious crime"*) e dovrebbe essere soggetto al preventivo esame di un giudice o di un organo indipendente.

Considerazioni finali

Le **due sentenze in commento, sebbene relative ad un sistema estraneo al nostro ordinamento giuridico**, rappresentano un ulteriore tassello attraverso il quale le Corti sovranazionali stanno delineando il **paradigma "europeo" degli istituti delle intercettazioni delle conversazioni e comunicazioni e dell'acquisizione dei dati relativi alle comunicazioni.**

La Corte EDU, infatti, ponendosi nel solco tracciato dalla giurisprudenza della Corte di Giustizia dell'Unione Europea in tema di acquisizione dei dati relativi alle comunicazioni elettroniche, ha affermato che l'esigenza di assicurare un costante equilibrio tra gli interessi pubblici sottesi all'impiego di tali strumenti e la tutela della riservatezza delle comunicazioni e della vita privata e familiare può essere assicurata solo dall'intervento di un **organo terzo e imparziale** che ne autorizzi l'impiego ovvero ne verifichi *ex post* la legittimità.

Di particolare rilievo, alla luce di quanto recentemente affermato dalla **Corte di Giustizia con la sentenza del 2 marzo 2021, C-746/18**, sono anche le affermazioni relative all'acquisizione diretta dei dati relativi alle comunicazioni presso i fornitori dei relativi servizi.

La lettura sinottica di tali pronunce potrebbe, dunque, essere di ausilio nella soluzione della questione ermeneutica nata proprio dalla citata sentenza della Corte di Giustizia dell'Unione Europea in merito alla **disapplicazione o meno dell'art. 132 d.lgs. 30 giugno 2003, n. 196,** quale immediata ricaduta di tale pronuncia, e, in caso positivo, alla procedura da applicare, sia pure in via analogica, in attesa dell'intervento del legislatore.

Al riguardo, infatti, sono affiorate nella giurisprudenza di merito diverse interpretazioni, ora a favore dell'immediata disapplicazione dell'art. 132 e

dell'applicabilità in via analogica degli artt. 266 e 267 cod. proc. pen. (come prospettato anche nel report sulla sentenza della Corte di Giustizia), ora, invece, contro tale disapplicazione, in considerazione del contenuto poco specifico della sentenza della Corte di Giustizia dell'Unione Europea. Sono state, infine, sottoposte ulteriori questioni pregiudiziali alla Corte di Giustizia in ordine alla efficacia *ex nunc* o *ex tunc* della pronuncia del 2 marzo scorso ed alla sua riferibilità anche all'ufficio del pubblico ministero che nell'ordinamento giuridico italiano si connota per l'autonomia e l'indipendenza dal potere esecutivo.

In attesa di una nuova pronuncia della Corte di Giustizia, nonché del probabile intervento del legislatore, anche questa Corte di cassazione potrebbe essere chiamata ad esaminare le ricadute della citata pronuncia della Corte di Giustizia del 2 marzo 2021 sul proprio – precedente orientamento ermeneutico in cui aveva ritenuto la compatibilità della disciplina italiana di conservazione dei dati di traffico – c.d. "*data retention"* – di cui all'art. 132, d.lgs 30 giugno 2003, n. 196, con le direttive n. 2002/58/CE e 2006/24/CE in tema di tutela della "*privacy*", come interpretate dalla giurisprudenza della Corte di Giustizia dell'Unione Europea (CGUE 8 aprile 2014, Digital Rights, C-293/12 e C-594/12; CGUE 21 dicembre 2016, Tele 2, C-203/15 e C-698/15) (Sez. 2,n. 5741 del 10/12/2019, dep. 2020, Dedej, Rv. 278568; Sez. 5, n. 33851 del 24/04/2018, Rv. 273892; Sez. 3, n. 48737 del 25/09/2019, Rv. 277353).